Secure Degrees of Freedom of One-Hop Wireless Networks With No Eavesdropper CSIT

Pritam Mukherjee, Jianwei Xie, and Sennur Ulukus, *Fellow, IEEE*

***Abstract*— We consider three channel models: the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, when no eavesdropper's channel state information (CSI) is available at the transmitters. In each case, we establish the optimal sum secure degrees of freedom (s.d.o.f.) by providing achievable schemes and matching converses. We show that the unavailability of the eavesdropper's channel state information at the transmitter (CSIT) does not reduce the s.d.o.f. of the wiretap channel with helpers. However, there is loss in s.d.o.f. for both the multiple access wiretap channel and the interference channel with an external eavesdropper. In particular, we show that in the absence of eavesdropper's CSIT, the K-user multiple access wiretap channel reduces to a wiretap channel with $(K-1)$ helpers from a sum s.d.o.f. perspective, and the optimal sum s.d.o.f. reduces from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ to $\frac{K-1}{2}$ in the absence of the eavesdropper's CSIT. Our results show that the lack of eavesdropper's CSIT does not have a significant impact on the optimal s.d.o.f. for any of the three channel models, especially when the number of users is large. This implies that physical layer security can be made robust to the unavailability of eavesdropper CSIT at high signal-to-noise ratio regimes by the careful modification of the achievable schemes as demonstrated in this paper.**

***Index Terms*— Wiretap channel, multiple access channel, interference channel, secure degrees of freedom, channel state information, cooperative jamming, interference alignment.**

I. Introduction

THE availability of channel state information at the transmitters (CSIT) plays a crucial role in securing wireless communication in the physical layer. In most practical scenarios, the channel gains are measured by the receivers and then fed back to the transmitters, which use the CSI to ensure security. A passive eavesdropper, however, cannot be expected to provide CSI for its channel. In this paper, we investigate how the unavailability of the eavesdropper's CSIT affects the optimal secure rates for three important channel models: the wiretap channel with helpers, the multiple access wiretap channel, and the interference channel with an external eavesdropper.

For each of these channel models, the secrecy capacity regions remain unknown, even with full eavesdropper CSIT. In the absence of exact capacity regions, we study the secure degrees of freedom (s.d.o.f.) of each channel model in the high signal-to-noise (SNR) regime. For the wiretap channel with M helpers and full eavesdropper CSIT, references [1], [2] determine the optimal s.d.o.f. to be $\frac{M}{M+1}$. Further, references [2], [3] determine the optimal sum s.d.o.f. for the K-user multiple access wiretap channel with full eavesdropper CSIT to be $\frac{K(K-1)}{K(K-1)+1}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. is shown to be $\frac{K(K-1)}{2K-1}$ in references [4], [5], with full eavesdropper CSIT. In this paper, we focus on the case when no eavesdropper CSIT is available. We show that for the wiretap channel with M helpers, an s.d.o.f. of $\frac{M}{M+1}$ is achievable even without eavesdropper's CSIT; thus, there is no loss of s.d.o.f. due to the unavailability of eavesdropper CSIT in this case. For the multiple access wiretap channel and the interference channel with an external eavesdropper, however, the optimal s.d.o.f. decreases when there is no eavesdropper CSIT. In particular, without eavesdropper CSIT, the K-user multiple access wiretap channel reduces to a wiretap channel with $(K-1)$ helpers and the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ to $\frac{K-1}{2}$ in the absence of eavesdropper CSIT.

In order to establish the optimal sum s.d.o.f., we propose achievable schemes and provide matching converse proofs for each of these channel models. We note that any achievable scheme for the wiretap channel with $(K-1)$ helpers is also an achievable scheme for the K-user multiple access wiretap channel. Further, a converse for the K-user multiple access wiretap channel is an upper bound for the wiretap channel with $(K-1)$ helpers as well. Thus, we provide achievable schemes for the wiretap channel with helpers and a converse for the multiple access wiretap channel. We consider both fixed and fading channel gains. For the wiretap channel with helpers and the multiple access wiretap channel, we present schemes based on real interference alignment [6] and vector space alignment [7] for fixed and fading channel gains, respectively. For

Manuscript received June 16, 2015; revised February 20, 2016 and August 13, 2016; accepted September 19, 2016. Date of publication October 19, 2016; date of current version February 14, 2017. This work was supported by NSF under Grant CNS 13-14733, Grant CCF 14-22111, and Grant CCF 14-22129. This paper was presented at the 2013 CISS, the 2015 IEEE ISIT, and the 2015 IEEE ITW.

P. Mukherjee and S. Ulukus are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: pritamm@umd.edu; ulukus@umd.edu).

J. Xie was with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. He is now with Google Inc, Mountain View, CA 94043 USA (e-mail: xiejw@umd.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2016.2618725

the interference channel, our achievable schemes are based on asymptotic real alignment [6], [8] and asymptotic vector space alignment [7] for fixed and fading channel gains, respectively. For every channel model, we design our achievable schemes such that, the structure of the real alignment based scheme for the case of fixed channel gains is similar to that of the vector space alignment based scheme for the case of fading channels. Thus, our achievable schemes indicate a loose correspondence between the real and vector space alignment techniques.

For the interference channel with an external eavesdropper, as in [5], every transmitter sacrifices a part of its message space to transmit cooperative jamming signals in the form of artificial noise. However, instead of one artificial noise block as in [5], our scheme requires two noise blocks from each transmitter. The $2K$ noise blocks from the K transmitters are then aligned at each legitimate receiver to occupy only $(K+1)$ *block dimensions* out of the full space of $2K$ dimensions, thus, achieving $\frac{K-1}{2K}$ s.d.o.f. per receiver. At the eavesdropper, however, the noise blocks do not align, and therefore, occupy the full space of $2K$ block dimensions, ensuring security of the message blocks. To the best of our knowledge, this is the first scheme in the literature which uses two noise blocks at each transmitter and aligns them in an optimal way to maximize the desired signal space at each legitimate receiver. An interesting aspect of our proposed schemes for the interference channel is that they provide confidentiality of the messages not only from the external eavesdropper but also from the unintended legitimate receivers. Thus, our schemes for both fixed and fading channel gains achieve the optimal sum s.d.o.f. for the K-user interference channel with both *confidential messages* and an external eavesdropper, with no eavesdropper CSIT.

To prove the converse, we combine techniques from [2], [5], and [9]. We exploit a key result in [9] that the output entropy at a receiver whose CSIT is not available is at least as large as the output entropy at a receiver whose CSIT is available, even when the transmitters cooperate and transmit correlated signals. This result is similar in spirit to the *least alignment lemma* in [10], where only *linear* transmission strategies are considered. Intuitively, no alignment of signals is possible at the receiver whose CSIT is unavailable; therefore, the signals occupy the maximum possible space at that receiver. We combine this insight with the techniques of [2] and [5]. Specifically, we use discretized versions of the *secrecy penalty lemma*, which quantifies the loss of rate due to the presence of an eavesdropper, and the *role of a helper lemma*, which captures the trade-off, arising out of decodability constraints, between the message rate and the entropy of an independent helper signal. Together, these techniques enable us to establish the optimal sum s.d.o.f. for the multiple access wiretap channel with no eavesdropper CSIT to be $\frac{K-1}{K}$ and the optimal sum s.d.o.f. for the interference channel with an external eavesdropper and no eavesdropper CSIT to be $\frac{K-1}{2}$.

A. Related Work

The secrecy capacity of the discrete memoryless wiretap channel is established in [11] and [12]. The s.d.o.f. of the single antenna Gaussian wiretap channel [13], and its variants [14]–[18] with different fading models and CSI availability conditions, is zero. In multi-user scenarios, however, positive s.d.o.f. values can be achieved. Each transmitters may have independent messages of its own, as in multiple access wiretap channels introduced in [19] and [20] and interference channels with confidential messages introduced in [21], or may act as helpers as in [22] and [23] . While cooperative jamming strategies can improve the achievable rates [19], i.i.d. Gaussian cooperative jamming signals limit the decoding performance of the legitimate receiver as well, and the s.d.o.f. achieved is still zero. Positive s.d.o.f. can be obtained by either structured signaling [24] or non-i.i.d. Gaussian signaling [25]. The exact optimal sum s.d.o.f. of the wiretap channel with M helpers and the K-user multiple access wiretap channel are established to be $\frac{M}{M+1}$ and $\frac{K(K-1)}{K(K-1)+1}$, respectively in [2], when full eavesdropper's CSIT is available. In this paper, we show that without eavesdropper's CSIT, the optimal s.d.o.f. for the wiretap channel with M helpers is still $\frac{M}{M+1}$, while the optimal sum s.d.o.f. of the K-user multiple access wiretap channel decreases to $\frac{K-1}{K}$.

The K-user interference channel with an external eavesdropper is studied in [26]. When the eavesdropper's CSIT is available, [26] proposes a scheme that achieves sum s.d.o.f. of $\frac{K-1}{2}$. The optimal s.d.o.f. in this case, however, is established in [5] to be $\frac{K(K-1)}{2K-1}$, using cooperative jamming signals along with interference alignment techniques. When the eavesdropper's CSIT is not available, reference [26] proposes a scheme that achieves a sum s.d.o.f. of $\frac{K-2}{2}$. In this paper, we establish the optimal s.d.o.f. in this case to be $\frac{K-1}{2}$.

A related line of research investigates the wiretap channel, the multiple access wiretap channel, and the broadcast channel with an *arbitrarily varying* eavesdropper [27]–[29], when the eavesdropper CSIT is not available. The eavesdropper's channel is assumed to be arbitrary, without any assumptions on its distribution, and security is guaranteed for *every* realization of the eavesdropper's channel. This models an exceptionally strong eavesdropper, which may control its own channel in an adversarial manner. Hence, the optimal sum s.d.o.f. is zero in each case with single antenna terminals, since the eavesdropper's channel realizations may be exactly equal to the legitimate user's channel realizations. On the other hand, in our model, the eavesdropper's channel gains are drawn from a known distribution, though the realizations are not known at the transmitters. We show that, with this mild assumption, strictly positive s.d.o.f. can be achieved even with single antennas at each transmitter and receiver for *almost all* channel realizations for helper, multiple access, and interference networks.

II. System Model and Definitions

In this paper, we consider three fundamental channel models: the wiretap channel with helpers, the multiple access wiretap channel, and the interference channel with an external eavesdropper. For each channel model, we consider two scenarios of channel variation: a) fixed channel gains, and b) fading channel gains. For the case of fixed channel gains, we assume that the channel gains are non-zero and have been drawn independently from a continuous distribution with

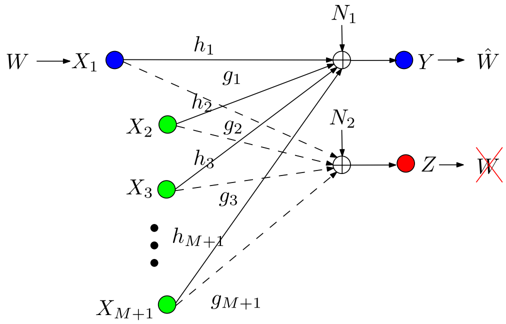

Fig. 1. Wiretap channel with M helpers.

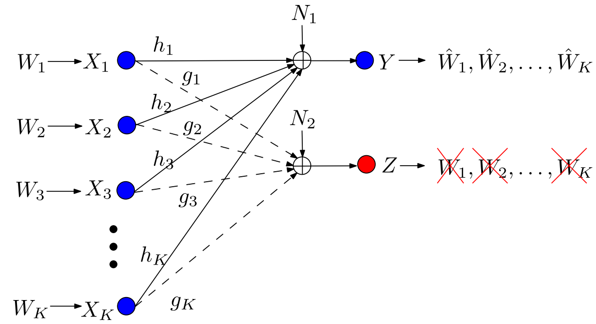

Fig. 2. K-user multiple access wiretap channel.

bounded support and remain fixed for the duration of the communication. On the other hand, in the fading scenario, we assume a fast fading model, where the channel gains vary in an i.i.d. fashion from one symbol period to another. In each symbol period, the channel gains are non-zero and are drawn from a common continuous distribution with bounded support. The common continuous distribution is known at all the terminals in the system. While we consider only real channel gains in this paper, we believe our results can be extended for complex channel gains; for further discussion, see [2, Sec. X].

Let Ω denote the collection of all channel gains in n channel uses. We assume full CSI at the receivers, that is, both the legitimates receivers and the eavesdropper know Ω. In the following subsections we describe each channel model and provide the relevant definitions.

A. Wiretap Channel With Helpers

The wiretap channel with M helpers, see Fig. 1, is described by,

$$Y(t) = h_1(t)X_1(t) + \sum_{i=2}^{M+1} h_i(t)X_i(t) + N_1(t) \tag{1}$$

$$Z(t) = g_1(t)X_1(t) + \sum_{i=2}^{M+1} g_i(t)X_i(t) + N_2(t) \tag{2}$$

where $X_1(t)$ denotes the channel input of the legitimate transmitter, and $Y(t)$ denotes the channel output at the legitimate receiver, at time t. $X(i), i = 2, \ldots, M+1$, are the channel inputs of the M helpers, and $Z(t)$ denotes the channel output at the eavesdropper, at time t. In addition, $N_1(t)$ and $N_2(t)$ are white Gaussian noise variables with zero-mean and unit-variance. Here, $h_i(t)$, $g_i(t)$ are the channel gains of the users to the legitimate receiver and the eavesdropper, respectively, and $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power constraint $\mathbb{E}[X_i(t)^2] \le P$, $i = 1, \ldots, M+1$.

The legitimate transmitter wishes to transmit a message W which is uniformly distributed in $\mathcal{W}$. A secure rate R, with $R = \frac{\log|\mathcal{W}|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W \neq \hat{W}] \le \epsilon_n$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W; Z^n, \Omega) \le \epsilon_n \tag{3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. The supremum of all achievable secure rates R is the secrecy capacity C_s and the s.d.o.f., d_s, is defined as

$$d_s = \lim_{P \to \infty} \frac{C_s}{\frac{1}{2}\log P} \tag{4}$$

B. Multiple Access Wiretap Channel

The K-user multiple access wiretap channel, see Fig. 2, is described by,

$$Y(t) = \sum_{i=1}^{K} h_i(t)X_i(t) + N_1(t) \tag{5}$$

$$Z(t) = \sum_{i=1}^{K} g_i(t)X_i(t) + N_2(t) \tag{6}$$

where $X_i(t)$ denotes the ith user's channel input, $Y(t)$ denotes the legitimate receiver's channel output, and $Z(t)$ denotes the eavesdropper's channel output, at time t. In addition, $N_1(t)$ and $N_2(t)$ are white Gaussian noise variables with zero-mean and unit-variance. Here, $h_i(t)$, $g_i(t)$ are the channel gains of the users to the legitimate receiver and the eavesdropper, respectively, and $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power constraint $\mathbb{E}[X_i(t)^2] \le P$, $i = 1, \ldots, K$.

The ith user transmits message W_i which is uniformly distributed in $\mathcal{W}_i$. A secure rate tuple $(R_1, \ldots, R_K)$, with $R_i = \frac{\log|\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W_i \neq \hat{W}_i] \le \epsilon_n$, for $i = 1, \ldots, K$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W^K; Z^n, \Omega) \le \epsilon_n \tag{7}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Here, W^K denotes the set of all the messages, i.e., $\{W_1, \ldots, W_K\}$. An s.d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if a rate tuple $(R_1, \ldots, R_K)$ is achievable with $d_i = \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}$. The sum s.d.o.f., d_s, is the largest achievable $\sum_{i=1}^{K} d_i$.

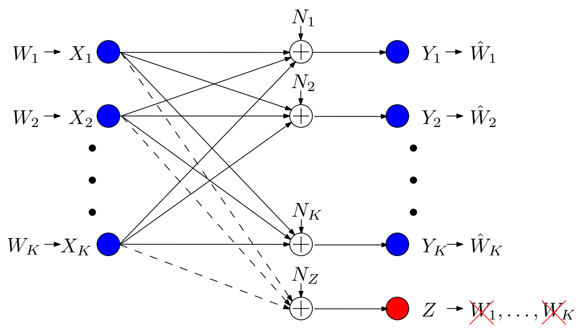

Fig. 3. K-user interference channel with an external eavesdropper.

C. Interference Channel With External Eavesdropper

The K-user interference channel with an external eavesdropper, see Fig. 3, is described by

$$Y_i(t) = \sum_{j=1}^{K} h_{ji}(t)X_j(t) + N_i(t), \quad i = 1, \ldots, K \tag{8}$$

$$Z(t) = \sum_{j=1}^{K} g_j(t)X_j(t) + N_Z(t) \tag{9}$$

where $Y_i(t)$ is the channel output of receiver i, $Z(t)$ is the channel output at the eavesdropper, $X_j(t)$ is the channel input of transmitter j, $h_{ji}(t)$ is the channel gain from transmitter j to receiver i, $g_j(t)$ is the channel gain from transmitter j to the eavesdropper, and $\{N_1(t), \ldots, N_K(t), N_Z(t)\}$ are mutually independent zero-mean unit-variance white Gaussian noise random variables, at time t. The channel gains to the eavesdropper, $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power constraint $\mathbb{E}[X_i(t)^2] \le P$, $i = 1, \ldots, K$.

Transmitter i wishes to send a message W_i, chosen uniformly from a set $\mathcal{W}_i$, to receiver i. The messages $W_1, \ldots, W_K$ are mutually independent. A secure rate tuple $(R_1, \ldots, R_K)$, with $R_i = \frac{\log|\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at all the legitimate receivers, namely, $\Pr[W_i \neq \hat{W}_i] \le \epsilon_n$, for $i = 1, \ldots, K$, and the security condition

$$\frac{1}{n} I(W^K; Z^n, \Omega) \le \epsilon_n \tag{10}$$

where $\epsilon_n \to 0$, as $n \to \infty$. An s.d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if a rate tuple $(R_1, \ldots, R_K)$ is achievable with $d_i = \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}$. The sum s.d.o.f., d_s, is the largest achievable $\sum_{i=1}^{K} d_i$.

III. Main Results and Discussion

In this section, we state the main results of this paper. We have the following theorems:

Theorem 1: For the wiretap channel with M helpers and no eavesdropper CSIT, the optimal sum s.d.o.f., d_s, is given by,

$$d_s = \frac{M}{M+1} \tag{11}$$

for fading channel gains and almost surely, for fixed channel gains.

Theorem 2: For the K-user multiple access wiretap channel with no eavesdropper CSIT, the optimal sum s.d.o.f., d_s, is given by,

$$d_s = \frac{K-1}{K} \tag{12}$$

for fading channel gains and almost surely, for fixed channel gains.

Theorem 3: For the K-user interference channel with an external eavesdropper with no eavesdropper CSIT, the optimal sum s.d.o.f., d_s, is given by,

$$d_s = \frac{K-1}{2} \tag{13}$$

for fading channel gains and almost surely, for fixed channel gains.

We present the proofs of Theorems 1 and 2 in Section IV and the proof of Theorem 3 in Section V. Let us first state a corollary obtained from Theorems 1 and 2, which establishes the entire s.d.o.f. region of the K-user multiple access wiretap channel with no eavesdropper CSIT.

Corollary 1: The s.d.o.f. region of the K-user multiple access wiretap channel with no eavesdropper CSIT is given by,

$$d_i \ge 0, \; i = 1, \ldots, K, \quad \text{and} \; \sum_{i=1}^{K} d_i \le \frac{K-1}{K} \tag{14}$$

The proof of Corollary 1 follows directly from Theorems 1 and 2. In particular, we can treat the K-user multiple access wiretap channel as a $(K-1)$ helper wiretap channel with transmitter i as the legitimate transmitter, and the remaining transmitters as helpers. This achieves the corner points $d_i = \frac{K-1}{K}$ and $d_j = 0$ for $j \neq i$ from Theorem 1. Therefore, given the sum s.d.o.f. upper bound in Theorem 2, and that each corner point with s.d.o.f. of $\frac{K-1}{K}$ for a single user is achievable, the region in Corollary 1 follows.

It is useful, at this point, to compare our results to the cases when the eavesdropper's CSI is available at the transmitter. Table I shows a comparison of the optimal s.d.o.f. values with and without eavesdropper CSIT. Interestingly, there is no loss in s.d.o.f. for the wiretap channel with helpers due to the absence of eavesdropper's CSIT.

However, for the multiple access wiretap channel and the interference channel with an external eavesdropper, the optimal s.d.o.f. decreases due to the unavailability of eavesdropper CSIT. For the multiple access wiretap channel, as the number of users, K increases, the optimal sum s.d.o.f. approaches 1 as $\sim \frac{1}{K^2}$ with eavesdropper's CSIT but only as $\sim \frac{1}{K}$ without eavesdropper's CSIT. Therefore, the loss of s.d.o.f. as a fraction of the optimal sum s.d.o.f. with eavesdropper CSIT is $\sim \frac{1}{K}$ for large K.

For the interference channel with an external eavesdropper too, there is a loss in s.d.o.f. due to the unavailability of the eavesdropper's CSIT. However, in this case, the optimal s.d.o.f. without eavesdropper CSIT closely tracks the s.d.o.f. with eavesdropper CSIT. In fact, it can be verified that the s.d.o.f. loss is bounded by $\frac{1}{4}$, which implies that the loss of

TABLE I
SUMMARY OF S.D.O.F. VALUES WITH AND WITHOUT EAVESDROPPER CSIT

Channel model	With Eve CSIT	Without Eve CSIT
Wiretap channel with M helpers	$\frac{M}{M+1}$	$\frac{M}{M+1}$
K-user multiple access wiretap channel	$\frac{K(K-1)}{K(K-1)+1}$	$\frac{K-1}{K}$
K-user interference channel with an external eavesdropper	$\frac{K(K-1)}{2K-1}$	$\frac{K-1}{2}$

s.d.o.f. as a fraction of the optimal s.d.o.f. with eavesdropper CSIT is $\sim \frac{1}{K}$ for large K, in this case also.

For the multiple access wiretap channel, we also consider the case where some of the transmitters have the eavesdropper's CSI. We state our achievable s.d.o.f. in this case in the following theorem.

Theorem 4: In the K-user MAC-WT, where $1 \leq m \leq K$ transmitters have eavesdropper CSI, and the remaining $K - m$ transmitters have no eavesdropper CSI, the following sum s.d.o.f. is achievable,

$$d_s = \frac{m(K-1)}{m(K-1)+1} \tag{15}$$

for fading channel gains and almost surely, for fixed channel gains.

We present the proof of Theorem 4 in Section VI. In this case, we note that when only one user has eavesdropper CSIT, i.e., $m = 1$, our achievable rate is the same as when no user has eavesdropper CSIT as in Theorem 2. On the other hand, when all users have eavesdropper CSIT, i.e., $m = K$, our achievable rate is the same as the optimal sum s.d.o.f. in [2]. We note that our achievable sum s.d.o.f. varies from the no eavesdropper CSIT result in Theorem 2 to the full eavesdropper CSIT sum s.d.o.f. in [2] as m increases from 1 to K.

IV. PROOFS OF THEOREMS 1 AND 2

First, we note that an achievable scheme for Theorem 1 implies an achievable scheme for Theorem 2, since the K-user multiple access wiretap channel may be treated as a wiretap channel with $(K-1)$ helpers. Further, we note that a converse for Theorem 2 suffices as a converse for Theorem 1. Thus, we will only provide achievable schemes for Theorem 1 and a converse proof for Theorem 2. An alternate converse for Theorem 1 also follows from the converse presented in [2] for the wiretap channel with M helpers and with eavesdropper CSIT, as the converse for the case of known eavesdropper CSIT serves as a converse for the case of unknown eavesdropper CSIT.

Next, we note that under our fixed and fading channel models, it suffices to provide an achievable scheme for the case of fixed channel gains and prove a converse for the case of fading channel gains. In general, the optimal sum s.d.o.f. d_s for fixed channel gains may depend on the channel realization, and we denote by $d_s^{fixed}(\boldsymbol{\omega})$, the optimal sum s.d.o.f. for the fixed channel realization $\boldsymbol{\omega} \triangleq (\boldsymbol{h}, \boldsymbol{g})$, where $\boldsymbol{h}$ and $\boldsymbol{g}$ denote the channel realizations of the legitimate receivers' channels and the eavesdropper's channel, respectively. We provide, in Section IV-A, a real alignment based achievable scheme for the wiretap channel with M helpers, and thus, show that the optimal sum s.d.o.f. $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all channel gains $\boldsymbol{\omega}$. Now, we show that

$$d_s^{var} \geq \mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})] \tag{16}$$

where d_s^{var} is the optimal sum s.d.o.f. in the fading channel gains case, by showing that a sum s.d.o.f. of $\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})]$ is achievable on the fading channel. To that end, we argue along the lines of [30]. Essentially, we quantize the (finite) range of each legitimate user's channel gain h_i, $i = 1, \ldots, K$ into m equal intervals $[h_i^k, h_i^{k+1})$, $k = 1, \ldots, m$. This results in the quantization of $\boldsymbol{h}$ into m^K rectangles $\mathcal{R}_j$, $j = 1, \ldots, m^K$. Let n_j be the number of channel uses when the channel realization $\boldsymbol{h} \in \mathcal{R}_j$. Due to the i.i.d. nature of channel variation, $\frac{n_j}{n} \to \mathbb{P}(\boldsymbol{h} \in \mathcal{R}_j)$, as $n \to \infty$. When the channel realization $\boldsymbol{h} \in \mathcal{R}_j$, one can achieve the s.d.o.f. given by $\operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g})$, almost surely, over n_j channel uses as $n_j \to \infty$, where ess inf denotes the essential infimum. Therefore, over n channel uses, one can achieve an s.d.o.f. of at least $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{P}(\boldsymbol{h} \in \mathcal{R}_j)$ which converges to $\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})]$ as $m \to \infty$, using the fact that $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{I}(\boldsymbol{h} \in \mathcal{R}_j)$ converges pointwise almost everywhere to $d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g})$, and noting that for each m, $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{I}(\boldsymbol{h} \in \mathcal{R}_j)$ is bounded by 1 for the multiple access wiretap channel.

Next, we prove the converse for the multiple access wiretap channel with fading channel gains in Section IV-B, and show that

$$d_s^{var} \leq \frac{K-1}{K} \tag{17}$$

Combining (16), (17) and the fact that $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all $\boldsymbol{\omega}$, we have

$$d_s^{var} = \frac{K-1}{K} \tag{18}$$

In order to determine the optimal sum s.d.o.f. in the fixed channel gains case, we first note using (16) and (18) that

$$\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})] \leq d_s^{var} = \frac{K-1}{K} \tag{19}$$

Combined with the fact that $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all channel gains $\boldsymbol{\omega}$, which follows from the achievable scheme

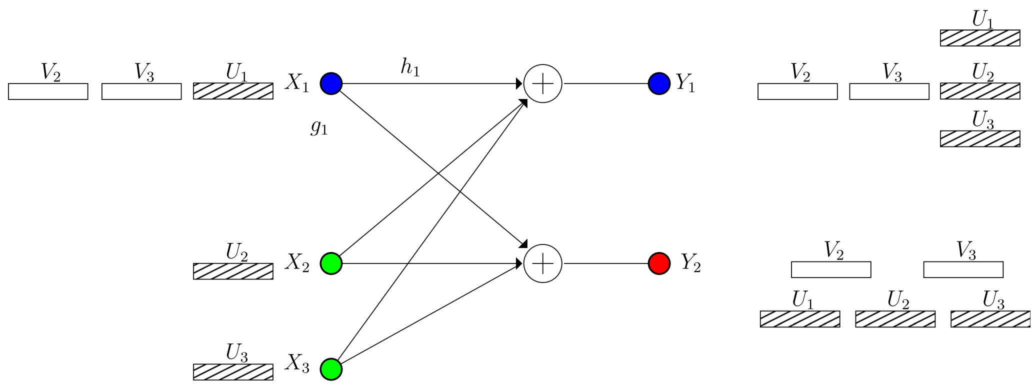

Fig. 4. Illustration of the alignment scheme for the Gaussian wiretap channel with M helpers with no eavesdropper CSI.

we provide in Section IV-A, we have that

$$d_s^{fixed}(\boldsymbol{\omega}) = \frac{K-1}{K} \tag{20}$$

for almost all channel gains $\boldsymbol{\omega}$.

Thus, the achievable scheme for the wiretap channel with M helpers and fixed channel gains in Section IV-A, and the converse for the multiple access wiretap channel with fading channel gains in Section IV-B suffice for the proofs of Theorems 1 and 2.

A. Achievability for the Wiretap Channel With Helpers

We now present achievable schemes for the wiretap channel with M helpers for fixed channel gains. We provide an achievable scheme for the case of fading channel gains in Appendix VII. Although one can utilize the achievable scheme developed for the fixed channel gains case on a symbol-by-symbol basis in the fading channel gains case, the alternative scheme provided in Appendix A is worth examining as it is designed to reveal similarities in the achievable schemes for the fixed and fading channel gains cases.

For fixed channels, we use the technique of real interference alignment [6], [8]. Let $\{V_2, V_3, \cdots, V_{M+1}, U_1, U_2, U_3, \cdots, U_{M+1}\}$ be mutually independent discrete random variables, each of which uniformly drawn from the same PAM constellation $C(a, Q)$

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{21}$$

where Q is a positive integer and a is a real number used to normalize the transmission power, and is also the minimum distance between the points belonging to $C(a, Q)$. Exact values of a and Q will be specified later. We choose the input signal of the legitimate transmitter as

$$X_1 = \frac{1}{h_1}U_1 + \sum_{k=2}^{M+1} \alpha_k V_k \tag{22}$$

where $\{\alpha_k\}_{k=2}^{M+1}$ are rationally independent among themselves and also rationally independent of all channel gains. The input signal of the jth helper, $j = 2, \cdots, M+1$, is chosen as

$$X_j = \frac{1}{h_j}U_j \tag{23}$$

Note that, neither the legitimate transmitter signal in (22) nor the helper signals in (23) depend on the eavesdropper CSI $\{g_k\}_{k=1}^{M+1}$. With these selections, observations of the receivers are given by,

$$Y = \sum_{k=2}^{M+1} h_1 \alpha_k V_k + \left(\sum_{j=1}^{M+1} U_j\right) + N_1 \tag{24}$$

$$Z = \sum_{k=2}^{M+1} g_1 \alpha_k V_k + \sum_{j=1}^{M+1} \frac{g_j}{h_j} U_j + N_2 \tag{25}$$

The intuition here is as follows: We use M independent sub-signals V_k, $k = 2, \cdots, M+1$, to represent the original message W. The input signal X_1 is a linear combination of V_ks and a jamming signal U_1. At the legitimate receiver, all of the cooperative jamming signals, U_ks, are aligned such that they occupy a small portion of the signal space. Since $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$ are rationally independent for all channel gains, except for a set of Lebesgue measure zero, the signals $\left\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=1}^{M+1} U_j\right\}$ can be distinguished by the legitimate receiver. This is similar to the case when there is full eavesdropper CSIT [2]. However, unlike the scheme in [2], we can no longer align signals at the eavesdropper due to lack of eavesdropper CSIT. Instead, we observe that $\left\{\frac{g_1}{h_1}, \cdots, \frac{g_{M+1}}{h_{M+1}}\right\}$ are rationally independent, and therefore, $\{U_1, U_2, \cdots, U_{M+1}\}$ *span* the *entire space* at the eavesdropper; see Fig. 4. Here, by the *entire space*, we mean the maximum number of *dimensions* that the eavesdropper is capable of decoding, which is $(M+1)$ in this case. Since the entire space at the eavesdropper is occupied by the cooperative jamming signals, the message signals $\{V_2, V_3, \cdots, V_{M+1}\}$ are secure, as we will mathematically prove in the sequel.

The following secrecy rate is achievable [12]

$$C_s \geq I(\mathbf{V}; Y) - I(\mathbf{V}; Z) \tag{26}$$

where $\mathbf{V} \triangleq \{V_2, V_3, \cdots, V_{M+1}\}$. Note that since $\boldsymbol{\Omega}$ is known at both the legitimate receiver and the eavesdropper, it can be considered to be an additional output at both the legitimate receiver and the eavesdropper. Further, since $\mathbf{V}$ is chosen to be independent of $\boldsymbol{\Omega}$, $\boldsymbol{\Omega}$ should appear in the conditioning of each of the mutual information quantities in (26). We keep this in mind, but drop it for the sake of notational simplicity.

First, we use Fano's inequality to bound the first term in (26). Note that the space observed at receiver 1 consists of $(2Q+1)^M(2MQ+2Q+1)$ points in $(M+1)$ dimensions, and the sub-signal in each dimension is drawn from a constellation of $C(a,(M+1)Q)$. Here, we use the property that $C(a,Q) \subset C(a,(M+1)Q)$. By using the Khintchine-Groshev theorem of Diophantine approximation in number theory [6], [8], we can bound the minimum distance d_{min} between the points in receiver 1's space as follows: For any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{((M+1)Q)^{M+\delta}} \tag{27}$$

for almost all rationally independent $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1,

$$\mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \tag{28}$$

$$\leq \exp\left(-\frac{a^2 k_\delta^2}{8((M+1)Q)^{2(M+\delta)}}\right) \tag{29}$$

where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P, then

$$\mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 (M+1)^2 P}{8((M+1)Q)^{2(M+\delta)+2}}\right) \tag{30}$$

$$= \exp\left(-\frac{k_\delta^2 \gamma^2 (M+1)^2 P^\delta}{8(M+1)^{2(M+1+\delta)}}\right) \tag{31}$$

and we can have $\mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose

$$\gamma \leq \min\left\{\left[\frac{1}{|h_1|} + \sum_{k=2}^{M+1}|\alpha_k|\right]^{-1}, |h_2|, |h_3|, \cdots, |h_{M+1}|\right\} \tag{32}$$

By Fano's inequality and the Markov chain $\mathbf{V} \to Y \to \hat{\mathbf{V}}$, we know that

$$H(\mathbf{V}|Y) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{33}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 (M+1)^2 P^\delta}{8(M+1)^{2(M+1+\delta)}}\right)\log(2Q+1)^M \tag{34}$$

$$= o(\log P) \tag{35}$$

where δ and γ are fixed, and $o(\cdot)$ is the little-o function. This means that

$$I(\mathbf{V};Y) = H(\mathbf{V}) - H(\mathbf{V}|Y) \tag{36}$$

$$\geq H(\mathbf{V}) - o(\log P) \tag{37}$$

$$= \log(2Q+1)^M - o(\log P) \tag{38}$$

$$\geq \log P^{\frac{M(1-\delta)}{2(M+1+\delta)}} - o(\log P) \tag{39}$$

$$= \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{40}$$

Next, we need to bound the second term in (26),

$$I(\mathbf{V};Z) = I(\mathbf{V},\mathbf{U};Z) - I(\mathbf{U};Z|\mathbf{V}) \tag{41}$$

$$= I(\mathbf{V},\mathbf{U};Z) - H(\mathbf{U}|\mathbf{V}) + H(\mathbf{U}|Z,\mathbf{V}) \tag{42}$$

$$= I(\mathbf{V},\mathbf{U};Z) - H(\mathbf{U}) + H(\mathbf{U}|Z,\mathbf{V}) \tag{43}$$

$$= h(Z) - h(Z|\mathbf{V},\mathbf{U}) - H(\mathbf{U}) + H(\mathbf{U}|Z,\mathbf{V}) \tag{44}$$

$$= h(Z) - h(N_2) - H(\mathbf{U}) + H(\mathbf{U}|Z,\mathbf{V}) \tag{45}$$

$$\leq h(Z) - h(N_2) - H(\mathbf{U}) + o(\log P) \tag{46}$$

$$\leq \frac{1}{2}\log P - \frac{1}{2}\log 2\pi e - \log(2Q+1)^{M+1} + o(\log P) \tag{47}$$

$$\leq \frac{1}{2}\log P - \frac{(M+1)(1-\delta)}{2(M+1+\delta)}\log P + o(\log P) \tag{48}$$

$$= \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{49}$$

where $\mathbf{U} \triangleq \{U_1, U_2, \cdots, U_{M+1}\}$, and (46) is due to the fact that given $\mathbf{V}$ and Z, the eavesdropper can decode $\mathbf{U}$ with probability of error approaching zero since $\left\{\frac{g_1}{h_1}, \cdots, \frac{g_{M+1}}{h_{M+1}}\right\}$ are rationally independent for all channel gains, except for a set of Lebesgue measure zero. Then, by Fano's inequality, $H(\mathbf{U}|Z,\mathbf{V}) \leq o(\log P)$ similar to the step in (35). In addition, $h(Z) \leq \frac{1}{2}\log P + o(\log P)$ in (47), since all the channel gains are drawn from a known distribution with bounded support.

Combining (40) and (49), we have

$$C_s \geq I(\mathbf{V};Y) - I(\mathbf{V};Z) \tag{50}$$

$$\geq \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{51}$$

$$= \frac{M-(2M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{52}$$

where again $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{M}{M+1}$ s.d.o.f. for this model where there is no eavesdropper CSI at the transmitters.

B. Converse for the Fading Multiple Access Wiretap Channel

We combine techniques from [2] and [9] to prove the converse. Here, we use $\mathbf{X}_i$ to denote the collection of all channel inputs $\{X_i(t),\ t = 1, \ldots, n\}$ of transmitter i. Similarly, we use $\mathbf{Y}$ and $\mathbf{Z}$ to denote the channel outputs at the legitimate receiver and the eavesdropper, respectively, over n channel uses. We further define $\mathbf{X}_1^K$ as the collection of all channel inputs from all of the transmitters, i.e., $\{\mathbf{X}_i,\ i = 1\ldots,K\}$. Finally, for a fixed j, we use $\mathbf{X}_{-j}$ to denote all channel inputs from all transmitters except transmitter j, i.e., $\{\mathbf{X}_i,\ i \neq j,\ i = 1\ldots, K\}$. Since all receivers know Ω, it appears in the conditioning in every entropy and mutual information term below. We keep this in mind, but drop it for the sake of notational simplicity. We divide the proof into three steps.

1) Deterministic Channel Model: We will show that there is no loss of s.d.o.f. in considering the following integer-input integer-output deterministic channel in (53)-(54) instead of the one in (5)-(6)

$$Y(t) = \sum_{i=1}^{K} \lfloor h_i(t) X_i(t) \rfloor \tag{53}$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor \tag{54}$$

with the constraint that

$$X_i \in \left\{0, 1, \ldots, \left\lfloor \sqrt{P} \right\rfloor\right\} \tag{55}$$

To that end, we will show that given any codeword tuple $(\mathbf{X}_1^G, \ldots, \mathbf{X}_K^G)$ for the original channel of (5)-(6), we can construct a codeword tuple $(\mathbf{X}_1^D, \ldots, \mathbf{X}_K^D)$ with $X_i^D(t) = \lfloor X_i^G(t) \rfloor \bmod \lfloor \sqrt{P} \rfloor$, for the deterministic channel of (53)-(54), that achieves an s.d.o.f. no smaller than the s.d.o.f. achieved by $(\mathbf{X}_1^G, \ldots, \mathbf{X}_K^G)$ on the original channel. Let us denote by $\mathbf{Y}^G$ and $\mathbf{Z}^G$, the outputs of the original channel of (5)-(6), when $(\mathbf{X}_1^G, \ldots, \mathbf{X}_K^G)$ is the input, that is,

$$Y^G(t) \triangleq \sum_{i=1}^{K} h_i(t) X_i^G(t) + N_1(t) \tag{56}$$

$$Z^G(t) \triangleq \sum_{i=1}^{K} g_i(t) X_i^G(t) + N_2(t) \tag{57}$$

Similarly, define

$$Y^D(t) \triangleq \sum_{i=1}^{K} \left\lfloor h_i(t) X_i^D(t) \right\rfloor \tag{58}$$

$$Z^D(t) \triangleq \sum_{i=1}^{K} \left\lfloor g_i(t) X_i^D(t) \right\rfloor \tag{59}$$

It suffices to show that

$$I(W_i; \mathbf{Y}^G) \leq I(W_i; \mathbf{Y}^D) + no(\log P) \tag{60}$$

$$I(W^K; \mathbf{Z}^D) \leq I(W^K; \mathbf{Z}^G) + no(\log P) \tag{61}$$

for every $i = 1, \ldots, K$. Here, (60) states that the information rate to the legitimate receiver in the discretized channel is at least as large as the information rate in the original Gaussian channel, and (61) states that the information leakage to the eavesdropper in the discretized channel is at most at the level of the information leakage in the original Gaussian channel, both of which quantified within a $o(\log P)$.

The proof of (60) follows along similar lines as the proof presented in [9] and [31]; we include a sketch here for completeness. First, note that there is no loss of d.o.f. due to integer inputs and outputs. To see this, define $\bar{Y}^D(t) = \sum_{i=1}^{K} \lfloor h_i(t) \lfloor X_i^G(t) \rfloor \rfloor$, and $E(t) = Y^G(t) - \bar{Y}^D(t)$. We have

$$\begin{aligned}
I(W_i; \boldsymbol{Y}^G|\Omega) &= I(W_i; \bar{\boldsymbol{Y}}^D + \boldsymbol{E}|\Omega) && (62)\\
&\leq I(W_i; \bar{\boldsymbol{Y}}^D, \boldsymbol{E}|\Omega) && (63)\\
&= I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + I(W_i; \boldsymbol{E}|\bar{\boldsymbol{Y}}^D, \Omega) && (64)\\
&\leq I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + h(\boldsymbol{E}|\Omega) \\
&\quad - h(\boldsymbol{E}|\bar{\boldsymbol{Y}}^D, W_i, \boldsymbol{X}_1^K, \Omega) && (65)\\
&\leq I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) - h(\boldsymbol{N}_1) \\
&\quad + \sum_{t=1}^{n} \mathbb{E}_\Omega \left[\frac{1}{2} \log\left(\sum_{i=1}^{K} (h_i(t)+1)^2 + 1\right)\right] && (66)\\
&\leq I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + no(\log P) && (67)
\end{aligned}$$

Next, we show that imposing per-symbol power constraints as in (55) does not incur any additional loss of d.o.f. It suffices to prove:

$$I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) - I(W_i; \boldsymbol{Y}^D|\Omega) \leq no(\log P) \tag{68}$$

We define $\hat{X}_i(t) = \lfloor X_i^G(t) \rfloor - X_i^D(t)$ and $\hat{Y} = \bar{Y}^D - Y^D$, and

$$\begin{aligned}
I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) &\leq I(W_i; \boldsymbol{Y}^D, \hat{\boldsymbol{Y}}|\Omega) && (69)\\
&\leq I(W_i; \boldsymbol{Y}^D|\Omega) + H(\hat{\boldsymbol{Y}}|\Omega) && (70)\\
&\leq I(W_i; \boldsymbol{Y}^D|\Omega) + \sum_{t=1}^{n} H(\hat{Y}(t)|\Omega) && (71)\\
&\leq I(W_i; \boldsymbol{Y}^D|\Omega) + \sum_{t=1}^{n}\sum_{i=1}^{K} H(\hat{X}_i(t)) + no(\log P) && (72)
\end{aligned}$$

Now, it can be shown that $H((\hat{X}_i(t)) \leq o(\log P)$ using the steps in [9, eqs. (138)–(158)]. Thus, (68) is proved. This concludes the sketch of proof of (60).

To prove (61), we first define

$$\bar{Z}(t) \triangleq \sum_{i=1}^{K} \left\lfloor g_i(t) \left\lfloor X_i^G(t) \right\rfloor \right\rfloor \tag{73}$$

$$\hat{Z}(t) \triangleq \bar{Z}(t) - Z^D(t) \tag{74}$$

$$\tilde{Z}(t) \triangleq \left\lfloor Z^G(t) \right\rfloor - \bar{Z}(t) - \lfloor N_2(t) \rfloor \tag{75}$$

Then, we have,

$$\begin{aligned}
I(W^K; \mathbf{Z}^D) &\leq I(W^K; \mathbf{Z}^D, \mathbf{Z}^G, \bar{\mathbf{Z}}) && (76)\\
&= I(W^K; \mathbf{Z}^G) + I(W^K; \bar{\mathbf{Z}}|\mathbf{Z}^G) \\
&\quad + I(W^K; \mathbf{Z}^D|\bar{\mathbf{Z}}, \mathbf{Z}^G) && (77)\\
&\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\mathbf{Z}^G) + H(\mathbf{Z}^D|\bar{\mathbf{Z}}, \mathbf{Z}^G) && (78)\\
&\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\lfloor \mathbf{Z}^G \rfloor) + H(\mathbf{Z}^D|\bar{\mathbf{Z}}) && (79)\\
&\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\bar{\mathbf{Z}} + \tilde{\mathbf{Z}} + \lfloor \mathbf{N}_2 \rfloor) + H(\hat{\mathbf{Z}}) && (80)
\end{aligned}$$

$$\leq I(W^K;\mathbf{Z}^G)+\sum_{t=1}^{n}H(\hat{Z}(t))$$
$$+\sum_{t=1}^{n}H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor) \quad (81)$$
$$\leq I(W^K;\mathbf{Z}^G)+no(\log P) \quad (82)$$

where $\lfloor \mathbf{Z}^G \rfloor = \left(\lfloor Z^G(1)\rfloor,\ldots,\lfloor Z^G(n)\rfloor\right)$. Here, (82) follows since $H(\hat{Z}(t)) \leq o(\log P)$ following the steps of the proof in [9, Appendix A.2]. In addition, recalling that Ω appears in the conditioning of each term in (81), note that $H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor,\Omega) \leq \mathbb{E}\left[H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor, g_1^K=\tilde{g}_1^K)\right]$. To bound this term, in going from (81) to (82), we have used the following lemma [32, Lemma E.1, Appendix E]

Lemma 1: Consider integer valued random variables x, r and s such that

$$x \perp r \quad (83)$$
$$s \in \{-L,\ldots,0,\ldots,L\} \quad (84)$$
$$\mathbb{P}(|r|\geq k) \leq e^{-f(k)} \quad (85)$$

for all positive k, for some integer L and a function $f(.)$. Let

$$y = x+r+s \quad (86)$$

Then,

$$H(x|y) \leq \log(2L+1)+2\log_2 e\left(\sum_{k=1}^{\infty} f(k)e^{-f(k)}\right)$$
$$+\frac{2L+1}{2}+N_f \quad (87)$$

where

$$N_f = \left|\left\{n\in\mathbb{Z}^+|e^{-f(n)}>\frac{1}{2}\right\}\right| \quad (88)$$

Note that, in our case, $\tilde{Z}(t)$ is integer valued and is bounded by $\sum_{i=1}^{K}\tilde{g}_i(t)+K+1$ for each realization $\tilde{g}_i(t)$ of $g_i(t)$, and we have

$$\mathbb{P}(|\lfloor N_2(t)\rfloor|>k) = \mathbb{P}(|N_2(t)-\{N_2(t)\}|>k) \quad (89)$$
$$\leq \mathbb{P}(|N_2(t)|+|\{N_2(t)\}|>k) \quad (90)$$
$$\leq \mathbb{P}(|N_2(t)|+1>k) \quad (91)$$
$$\leq e^{\frac{(k-1)^2}{2}} \quad (92)$$

Thus, using the choice $f(k)=\frac{(k-1)^2}{2}$, N_f is clearly bounded and thus, $H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor,\Omega) \leq o(\log P)$, which is the step going from (81) to (82).

Therefore, the s.d.o.f. of the deterministic channel in (53)-(54) with integer channel inputs as described in (55) is no smaller than the s.d.o.f. of the original channel in (5)-(6). Consequently, any upper bound (e.g., converse) developed for the s.d.o.f. of (53)-(54) will serve as an upper bound for the s.d.o.f. of (5)-(6). Thus, we will consider this deterministic channel in the remaining part of the converse.

2) An Upper Bound on the Sum Rate: We begin as in the *secrecy penalty lemma* in [2], i.e., [2, Lemma 1]. Note that, unlike [2, Lemma 1], channel inputs are integer here and satisfy (55):

$$n\sum_{i=1}^{K}R_i \leq I(W^K;\mathbf{Y})-I(W^K;\mathbf{Z})+n\epsilon \quad (93)$$
$$\leq I(W^K;\mathbf{Y}|\mathbf{Z})+n\epsilon \quad (94)$$
$$\leq I(\mathbf{X}_1^K;\mathbf{Y}|\mathbf{Z})+n\epsilon \quad (95)$$
$$\leq H(\mathbf{Y}|\mathbf{Z})+n\epsilon \quad (96)$$
$$= H(\mathbf{Y},\mathbf{Z})-H(\mathbf{Z})+n\epsilon \quad (97)$$
$$\leq H(\mathbf{X}_1^K,\mathbf{Y},\mathbf{Z})-H(\mathbf{Z})+n\epsilon \quad (98)$$
$$= H(\mathbf{X}_1^K)-H(\mathbf{Z})+n\epsilon \quad (99)$$
$$\leq \sum_{k=1}^{K}H(\mathbf{X}_k)-H(\mathbf{Z})+n\epsilon \quad (100)$$

where (99) follows since $H(\mathbf{Y},\mathbf{Z}|\mathbf{X}_1^K)=0$ for the channel in (53)-(54). Also, to ensure decodability at the legitimate receiver, we use the *role of a helper lemma* in [2], i.e., [2, Lemma 2],

$$n\sum_{i\neq j}R_i \leq I(W_{-j};\mathbf{Y})+n\epsilon' \quad (101)$$
$$\leq I(\mathbf{X}_{-j};\mathbf{Y})+n\epsilon' \quad (102)$$
$$= H(\mathbf{Y})-H(\mathbf{Y}|\mathbf{X}_{-j})+n\epsilon' \quad (103)$$
$$= H(\mathbf{Y})-H\left(\sum_{i=1}^{K}\lfloor\mathbf{h}_i\mathbf{X}_i\rfloor|\mathbf{X}_{-j}\right)+n\epsilon' \quad (104)$$
$$= H(\mathbf{Y})-H(\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)+n\epsilon' \quad (105)$$
$$= H(\mathbf{Y})-H(\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor,\mathbf{X}_j)+H(\mathbf{X}_j|\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)$$
$$+n\epsilon' \quad (106)$$
$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)+H(\mathbf{X}_j|\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)+n\epsilon' \quad (107)$$
$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)$$
$$+\sum_{t=1}^{n}H(X_j(t)|\lfloor h_j(t)X_j(t)\rfloor)+n\epsilon' \quad (108)$$
$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)+n\epsilon'+nc \quad (109)$$

where $\mathbf{h}_j\mathbf{X}_j \stackrel{\Delta}{=} \left\{h_j(t)X_j(t), t=1,\ldots,n\right\}$, and recalling that Ω appears in the conditioning of each term in (108), (109) follows using the following lemma.

Lemma 2: Let X be an integer valued random variable satisfying (55)*, and h be drawn from a distribution $F(h)$ satisfying $\int_{-\infty}^{\infty}\log\left(1+\frac{1}{|h|}\right)dF(h)\leq c$ for some $c\in\mathbb{R}$. Then,*

$$H(X|\lfloor hX\rfloor,h) \leq c \quad (110)$$

The proof of this lemma is presented in Appendix C. The constraint imposed in Lemma 2 is a mild technical condition. A sufficient condition for satisfying the constraint is that there exists an $\epsilon>0$ such that the probability density function (pdf) is bounded in the interval $(-\epsilon,\epsilon)$. This is due to the fact that

$\log\left(1+\frac{1}{|h|}\right) \leq \log\left(1+\frac{1}{|\epsilon|}\right)$, when $|h| > \epsilon$ and following:

$$\int_{-\epsilon}^{\epsilon} f(h)\log\left(1+\frac{1}{|h|}\right)dh \leq M\int_{-\epsilon}^{\epsilon}\log\left(1+\frac{1}{|h|}\right)dh \tag{111}$$

$$\leq 2M\left[\int_0^{\epsilon}\log(1+h)\,dh + \int_0^{\epsilon}|\log h|dh\right] \tag{112}$$

$$\leq c \tag{113}$$

where $f(h) \leq M$ on $(-\epsilon, \epsilon)$, and the last step follows since both integrals in (112) are bounded. Most common distributions such as Gaussian, exponential and Laplace satisfy this condition.

Eliminating $H(\mathbf{X}_j)$s using (100) and (109), we get,

$$Kn\sum_{i=1}^{K} R_i \leq KH(\mathbf{Y}) - H(\mathbf{Z}) + nK(\epsilon' + c) + n\epsilon \tag{114}$$

$$\leq (K-1)\frac{n}{2}\log P + (H(\mathbf{Y}) - H(\mathbf{Z})) + n\epsilon'' \tag{115}$$

where $\epsilon'' = o(\log P)$. Dividing by n and letting $n \to \infty$,

$$K\sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2}\log P + \epsilon'' + \lim_{n\to\infty}\frac{1}{n}(H(\mathbf{Y}) - H(\mathbf{Z})) \tag{116}$$

Now dividing by $\frac{1}{2}\log P$ and taking $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K} + \frac{1}{K}\lim_{P\to\infty}\lim_{n\to\infty}\frac{H(\mathbf{Y}) - H(\mathbf{Z})}{\frac{n}{2}\log P} \tag{117}$$

3) Bounding the Difference of Entropies: We now upper bound the difference of entropies $H(\mathbf{Y}) - H(\mathbf{Z})$ in (117) as:

$$H(\mathbf{Y}) - H(\mathbf{Z}) \leq \sup_{\{\mathbf{X}_i\}:\mathbf{X}_i \perp\!\!\!\perp \mathbf{X}_j} H(\mathbf{Y}) - H(\mathbf{Z}) \tag{118}$$

$$\leq \sup_{\{\mathbf{X}_i\}} H(\mathbf{Y}) - H(\mathbf{Z}) \tag{119}$$

where $X \perp\!\!\!\perp Y$ is used to denote that X and Y are statistically independent and (119) follows from (118) by relaxing the condition of independence in (118). Since the $\mathbf{X}_i$s in (119) may be arbitrarily correlated, we can think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}) - H(\mathbf{Z})$, where $\mathbf{Y}$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. This brings us to the K-user MISO broadcast channel setting of [9], where it is shown that the difference of entropies, $H(\mathbf{Y}) - H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver are unknown, even without security constraints. Indeed, we have the following lemma.

Lemma 3: For the deterministic channel model stated in (53)-(55)*, with the channel gains to* $\mathbf{Z}$ *unknown at the transmitter, we have*

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq no(\log P) \tag{120}$$

The proof of Lemma 3 follows along the lines of [9, eqs. (75)–(103)]; in order to make our proof self-contained,[1] we provide a sketch of the relevant steps in Appendix D.

Using (120) in (117), we have

$$\sum_{i=1}^{K} d_i \leq \tfrac{K-1}{K} \tag{121}$$

This completes the converse proof of Theorem 2.

V. Proof of Theorem 3

In this section, we present the proof of Theorem 3. We first present separate achievable schemes for fixed and fading channel gains and then present the converse. For the interference channel, we require asymptotic schemes with both real [8], and vector space alignment [7] techniques. The converse combines techniques from [4] and [9].

A. Achievability for the Interference Channel

An achievable scheme for the interference channel with an external eavesdropper and no eavesdropper CSIT is presented in [26, Th. 3]. That scheme achieves sum s.d.o.f. of $\frac{K-2}{2}$. Here, we present the optimal schemes which achieve $\frac{K-1}{2}$ sum s.d.o.f for fixed channel gains. In this section, we focus on the case when $K = 3$, which highlights the main ideas of the general K-user scheme for fixed channel gains. We present a corresponding vector space alignment scheme for fading channel gains in Appendix E. We present the general K-user schemes for both fixed and fading channel gains in Appendix F. As in the achievability for the wiretap channel with helpers, we use real interference alignment techniques for fixed channel gains. However, unlike the case of wiretap channel with helpers, we need to use asymptotic alignment in each case.

We use the technique of asymptotic real interference alignment introduced in [8]. Fig. 5 shows the desired signal alignment at the receivers and the eavesdropper. In the figure, the boxes labeled by V denote the message symbols, while the hatched boxes labeled with U denote artificial noise symbols. We observe from Fig. 5 that 4 out of 6 *signal dimensions* are buried in the artificial noise. Thus, heuristically, the s.d.o.f. for each legitimate user pair is $\frac{2}{6} = \frac{1}{3}$, and the sum s.d.o.f. is, therefore, $3 \times \frac{1}{3} = 1$, as expected from our optimal sum s.d.o.f. expression $\frac{K-1}{2} = \frac{3-1}{2} = 1$.

In the K-user case, we have a similar alignment scheme. Each transmitter sends two artificial noise blocks along with $(K-1)$ message blocks. At each legitimate receiver, the $2K$ noise blocks from the K transmitters align such that they occupy only $(K+1)$ *block dimensions*. This is done by aligning $\tilde{U}_k$ with U_{k+1} for $k = 1, \ldots, (K-1)$, at each legitimate receiver. The unintended messages at each legitimate receiver are aligned underneath the $(K+1)$ artificial noise dimensions. To do so, we use two main ideas. First, two blocks from the same transmitter cannot be aligned at *any* receiver. This

[1] Based on the suggestion of an anonymous reviewer.

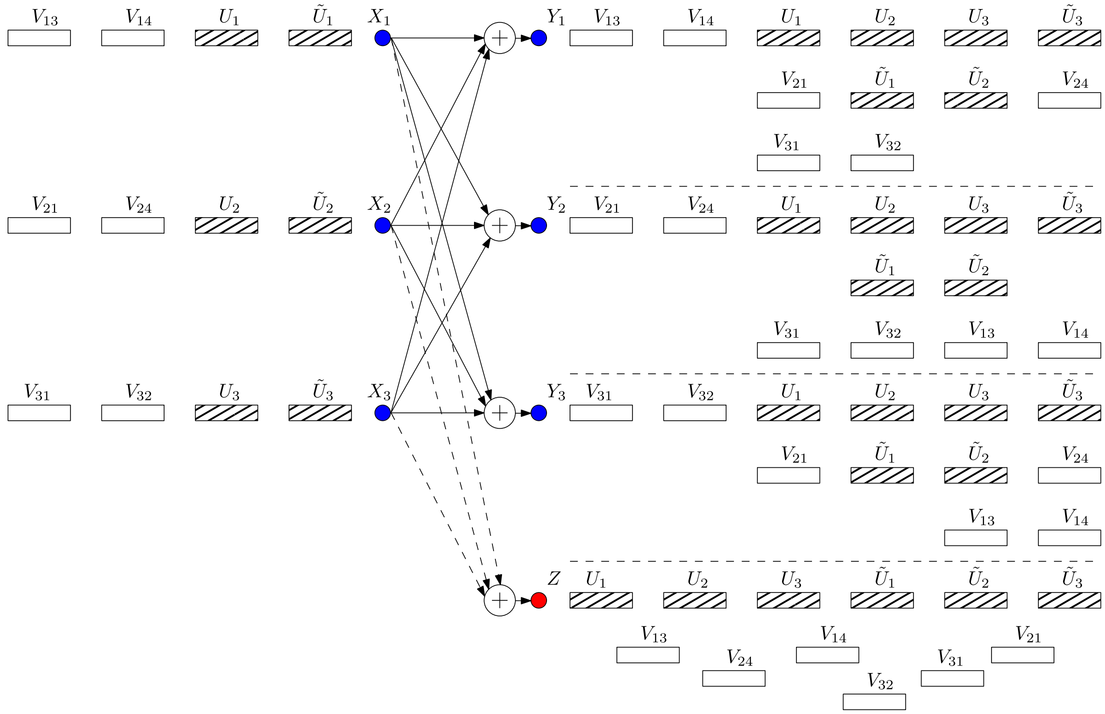

Fig. 5. Alignment for the interference channel with $K = 3$.

is because if two blocks from the same transmitter align at any receiver, they align at every other receiver as well, which is clearly not desirable. Secondly, each message block aligns with the same artificial noise block at every unintended receiver. Thus, in Fig. 5, V_{21} and V_{24} appear in different columns at each receiver. Further, V_{21} appears underneath U_1 at both of the unintended legitimate receivers 1 and 2. It can be verified that these properties hold for every message block. As an interesting by-product, this alignment scheme provides confidentiality of the unintended messages at the legitimate transmitters for free. The $(K-1)$ intended message blocks at a legitimate receiver occupy distinct block dimensions; thus, achieving a d.o.f. of $\frac{K-1}{2K}$ for each transmitter-receiver pair. At the eavesdropper, no alignment is possible since its CSIT is unavailable. Thus, the $2K$ artificial noise blocks occupy the full space of $2K$ block dimensions. This ensures security of the messages at the eavesdropper.

Note that we require two artificial noise blocks to be transmitted from each transmitter. When the eavesdropper CSIT is available, the optimal achievable scheme, presented in [5], requires one artificial noise block from each transmitter; the K noise blocks from the K transmitters are aligned with the messages at the eavesdropper in order to ensure security. In our case, however, the eavesdropper's CSIT is not available. Thus, in order to guarantee security, we need a total of $2K$ noise blocks to occupy the full space of $2K$ block dimensions at the eavesdropper. This is achieved by sending two artificial noise blocks from each transmitter. Further, to achieve an s.d.o.f. of $\frac{K-1}{2K}$ per user pair, we need to create $(K-1)$ noise-free message block dimensions at each legitimate receiver. We ensure this by systematically aligning the $2K$ noise symbols to occupy only $(K+1)$ block dimensions at each legitimate receiver. To the best of our knowledge, this is the first achievable scheme in the literature that uses two artificial noise blocks from each transmitter and then aligns them to maximize the noise-free message dimensions at each legitimate receiver.

Let us now present the 3-user scheme in more detail. Let m be a large integer. Also, let c_1, c_2, c_3 and c_4 be real constants drawn from a fixed continuous distribution with bounded support independently of each other and of all the channel gains. This ensures that the c_is are *rationally independent* of each other and of the channel gains. Now, we define four sets T_i, $i = 1, \dots, 4$, as follows:

$$T_1 \triangleq \Big\{h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{32}} c_1^s : r_{jk}, s \in \{1, \dots, m\}\Big\} \tag{122}$$

$$T_2 \triangleq \left\{h_{21}^{r_{21}} h_{22}^{r_{22}} h_{23}^{r_{23}} \left(\frac{h_{12}}{h_{11}}\right)^{r_{12}} \left(\frac{h_{13}}{h_{11}}\right)^{r_{13}} h_{31}^{r_{31}} h_{32}^{r_{32}} c_2^s : r_{jk}, s \in \{1, \dots, m\}\right\} \tag{123}$$

$$T_3 \triangleq \left\{h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} \left(\frac{h_{21}}{h_{22}}\right)^{r_{21}} \left(\frac{h_{23}}{h_{22}}\right)^{r_{23}} h_{12}^{r_{12}} h_{13}^{r_{13}} c_3^s : r_{jk}, s \in \{1, \dots, m\}\right\} \tag{124}$$

$$T_4 \triangleq \Big\{h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} h_{21}^{r_{21}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{23}^{r_{23}} c_4^s : r_{jk}, s \in \{1, \dots, m\}\Big\} \tag{125}$$

Let M_i be the cardinality of the set T_i. Note that all the M_is are the same, which we denote by M, which is given as,

$$M \triangleq m^8 \tag{126}$$

We subdivide each message W_i into 2 independent sub-messages V_{ij}, $j = 1, \ldots, 4$, $j \neq i, i+1$. For each transmitter i, let $\mathbf{p}_{ij}$ be the vector containing all the elements of T_j, for $j \neq i, i+1$. For any given (i, j) with $j \neq i, i+1$, $\mathbf{p}_{ij}$ represents the dimension along which message V_{ij} is sent. Further, at each transmitter i, let $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ be vectors containing all the elements in sets T_i and $\beta_i T_{i+1}$, respectively, where

$$\beta_i = \begin{cases} \frac{1}{h_{ii}}, & \text{if } i = 1, 2 \\ 1, & \text{if } i = 3 \end{cases} \tag{127}$$

The vectors $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ represent dimensions along which artificial noise symbols U_i and $\tilde{U}_i$, respectively, are sent. We define a $4M$ dimensional vector $\mathbf{b}_i$ by stacking the $\mathbf{p}_{ij}$s, $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ as

$$\mathbf{b}_i^T = \begin{bmatrix} \mathbf{p}_{i1}^T \ldots \mathbf{p}_{i(i-1)}^T & \mathbf{p}_{i(i+2)}^T \ldots \mathbf{p}_{i4} & \mathbf{q}_i & \tilde{\mathbf{q}}_i \end{bmatrix} \tag{128}$$

The transmitter encodes V_{ij} using an M dimensional vector $\mathbf{v}_{ij}$, and the cooperative jamming signals U_i and $\tilde{U}_i$ using M dimensional vectors $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. Each element of $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$ are drawn in an i.i.d. fashion from $C(a, Q)$ in (21). Let

$$\mathbf{a}_i^T = \begin{bmatrix} \mathbf{v}_{i1}^T \ldots \mathbf{v}_{i(i-1)}^T & \mathbf{v}_{i(i+2)}^T \ldots \mathbf{v}_{i4} & \mathbf{u}_i & \tilde{\mathbf{u}}_i \end{bmatrix} \tag{129}$$

The channel input of transmitter i is then given by

$$x_i = \mathbf{a}_i^T \mathbf{b}_i \tag{130}$$

Let us now analyze the structure of the received signals at the receivers. For example, consider receiver 1. The desired signals at receiver 1, $\mathbf{v}_{13}$ and $\mathbf{v}_{14}$ arrive along dimensions $h_{11}T_3$ and $h_{11}T_4$, respectively. Since only T_i (and not T_j, $j \neq i$) contains c_i, these dimensions are rationally independent. Thus, they appear along different columns in Fig. 5. The artificial noise symbols $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ and $\tilde{\mathbf{u}}_3$ arrive along dimensions $h_{11}T_1$, $h_{21}T_2$, $h_{31}T_3$ and $h_{31}T_4$, respectively. Again they are all rationally separate and thus, appear along different columns in Fig. 5. Further, they are all separate from the dimensions of the desired signals, because T_3 and T_4 do not contain h_{11}, while T_1 and T_2 do not contain either c_3 or c_4. On the other hand, the unintended signals $\mathbf{v}_{21}$ and $\mathbf{v}_{31}$ arrive along $h_{21}T_1$ and $h_{31}T_1$, and since T_1 contains powers of h_{21} and h_{31}, they align with the artificial noise $\mathbf{u}_1$ in $\tilde{T}_1$, where,

$$\tilde{T}_1 \triangleq \{h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{32}} c_1^s : r_{jk}, s \in \{1, \ldots, m+1\}\} \tag{131}$$

Similarly, we define

$$\tilde{T}_2 \triangleq \left\{ h_{21}^{r_{21}} h_{22}^{r_{22}} h_{23}^{r_{23}} \left(\frac{h_{12}}{h_{11}}\right)^{r_{12}} \left(\frac{h_{13}}{h_{11}}\right)^{r_{13}} h_{31}^{r_{31}} h_{32}^{r_{32}} c_2^s : r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{132}$$

$$\tilde{T}_3 \triangleq \left\{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} \left(\frac{h_{21}}{h_{22}}\right)^{r_{21}} \left(\frac{h_{23}}{h_{22}}\right)^{r_{23}} h_{12}^{r_{12}} h_{13}^{r_{13}} c_3^s : r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{133}$$

$$\tilde{T}_4 \triangleq \{h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} h_{21}^{r_{21}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{23}^{r_{23}} c_4^s : r_{jk}, s \in \{1, \ldots, m+1\}\} \tag{134}$$

We note that the unintended signals $\mathbf{v}_{32}$ and $\mathbf{v}_{24}$ arrive along $h_{31}T_2$ and $h_{21}T_4$ and thus, align with $\mathbf{u}_2$ and $\tilde{\mathbf{u}}_3$, respectively, in $\tilde{T}_2$ and $\tilde{T}_4$. Thus, they appear in the same column in Fig.5. Finally, the artificial noise symbols $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ align with $\mathbf{u}_2$ and $\mathbf{u}_3$, respectively.

At receiver 2, the desired signals $\mathbf{v}_{21}$ and $\mathbf{v}_{24}$ arrive along rationally independent dimensions $h_{22}T_1$ and $h_{22}T_4$, respectively. The artificial noise symbols $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ and $\tilde{\mathbf{u}}_3$ arrive along dimensions $h_{12}T_1$, $h_{22}T_2$, $h_{32}T_3$ and $h_{32}T_4$, respectively. Thus, they lie in dimensions $\tilde{T}_1$, $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$, respectively. They are all separate from the dimensions of the desired signals, because $\tilde{T}_1$ and $\tilde{T}_4$ do not contain h_{22}, while $\tilde{T}_2$ and $\tilde{T}_3$ do not contain either c_1 or c_4. The artificial noise symbols $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ arrive along dimensions $\left(\frac{h_{12}}{h_{11}}\right) T_2$ and T_3, respectively; thus, they align with $\mathbf{u}_2$ and $\mathbf{u}_3$ in $\tilde{T}_2$ and $\tilde{T}_3$, respectively. The unintended signals $\mathbf{v}_{13}$ and $\mathbf{v}_{14}$ arrive along $h_{12}T_3$ and $h_{12}T_4$, respectively, and lie in $\tilde{T}_3$ and $\tilde{T}_4$, respectively. Similarly, $\mathbf{v}_{31}$ and $\mathbf{v}_{32}$ lie in $\tilde{T}_1$ and $\tilde{T}_2$, respectively. A similar analysis is true for receiver 3 as well.

At the eavesdropper, there is no alignment, since the channel gains of the eavesdropper are not known at the transmitters. In fact, the artificial noise symbols all arrive along different dimensions at the receiver. Thus, heuristically, they exhaust the decoding capability of the eavesdropper almost completely.

We note that the interference at each receiver is confined to the dimensions $\tilde{T}_1$, $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$. Further, these dimensions are separate from the dimensions occupied by the desired signals at each receiver. Specifically, at receiver i, the desired signals occupy dimensions $h_{ii}T_j$, $j \neq i, i+1$. These dimensions are separate from $\tilde{T}_i$ and $\tilde{T}_{i+1}$, since only T_j contains powers of c_j. Further, $\tilde{T}_j$, $j \neq i, i+1$ do not contain powers of h_{ii}. Thus, the set

$$S = \left(\bigcup_{j \neq i, i+1} h_{ii} T_j \right) \bigcup \left(\bigcup_{j=1}^{4} \tilde{T}_j \right) \tag{135}$$

has cardinality

$$M_S = 2m^8 + 4(m+1)^8 \tag{136}$$

Intuitively, out of these M_S dimensions, $2m^8$ dimensions carry the desired signals. Thus, the s.d.o.f. of each legitimate user pair is $\frac{2m^8}{2m^8+4(m+1)^8}$ which approaches $\frac{1}{3}$ as $m \to \infty$. Thus, the sum s.d.o.f. is 1. We omit the formal calculation of the achievable rate here and instead present it in Appendix F-A for the general K-user case. Further, note that the unintended messages at each receiver are buried in artificial noise, see Fig. 5. Thus, our scheme provides confidentiality of messages from unintended legitimate receivers as well.

B. Converse for the Interference Channel

The steps of the converse are similar to that of the proof in Section IV-B. The notation here is also the same as in Section IV-B. Again, we divide the proof into three steps.

1) Deterministic Channel Model: We consider the deterministic channel given as,

$$Y_k(t) = \sum_{i=1}^{K} \lfloor h_{ik}(t) X_i(t) \rfloor \tag{137}$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor \tag{138}$$

for $k = 1, \ldots, K$, with the constraint that

$$X_i(t) \in \left\{0, 1, \ldots, \left\lfloor \sqrt{P} \right\rfloor \right\} \tag{139}$$

We can show that there is no loss of s.d.o.f. in considering the channel in (137)-(138) instead of the one in (8)-(9), as in Section IV-B.1. Thus, we will consider this deterministic channel in the remaining part of the converse. Since all receivers know Ω, it appears in the conditioning in every entropy and mutual information term below. We keep this in mind, but drop it for the sake of notational simplicity.

2) An Upper Bound on the Sum Rate: We begin as in the *secrecy penalty lemma* in [2], i.e., [2, Lemma 1]. Note that, unlike [2, Lemma 1], channel inputs are integer here:

$$\begin{aligned}
n\sum_{i=1}^{K} R_i &\le I(W^K; \mathbf{Y}_1^K) - I(W^K; \mathbf{Z}) + n\epsilon && (140)\\
&\le I(W^K; \mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon && (141)\\
&\le I(\mathbf{X}_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon && (142)\\
&\le H(\mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon && (143)\\
&= H(\mathbf{Y}_1^K, \mathbf{Z}) - H(\mathbf{Z}) + n\epsilon && (144)\\
&\le H(\mathbf{X}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - H(\mathbf{Z}) + n\epsilon && (145)\\
&= H(\mathbf{X}_1^K) - H(\mathbf{Z}) + n\epsilon && (146)\\
&\le \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) + n\epsilon && (147)
\end{aligned}$$

where (146) follows since $H(\mathbf{Y}_1^K, \mathbf{Z}|\mathbf{X}_1^K) = 0$ for the channel in (137)-(138).

Also, to ensure decodability at the legitimate receiver, we use the *role of a helper lemma* in [2], i.e., [2, Lemma 2],

$$\begin{aligned}
nR_i &\le I(W_i; \mathbf{Y}_i) + n\epsilon' && (148)\\
&\le I(\mathbf{X}_i; \mathbf{Y}_i) + n\epsilon' && (149)\\
&= H(\mathbf{Y}_i) - H(\mathbf{Y}_i|\mathbf{X}_i) + n\epsilon' && (150)\\
&= H(\mathbf{Y}_i) - H(\left\lfloor \mathbf{h}_j \mathbf{X}_j \right\rfloor) + n\epsilon' && (151)\\
&= H(\mathbf{Y}_i) - H(\left\lfloor \mathbf{h}_j \mathbf{X}_j \right\rfloor, \mathbf{X}_j) + H(\mathbf{X}_j| \left\lfloor \mathbf{h}_j \mathbf{X}_j \right\rfloor) \\
&\quad + n\epsilon' && (152)\\
&\le H(\mathbf{Y}_i) - H(\mathbf{X}_j) + H(\mathbf{X}_j| \left\lfloor \mathbf{h}_j \mathbf{X}_j \right\rfloor) + n\epsilon' && (153)\\
&\le H(\mathbf{Y}_i) - H(\mathbf{X}_j) + \sum_{t=1}^{n} H(X_j(t)| \left\lfloor h_j(t) X_j(t) \right\rfloor) \\
&\quad + n\epsilon' && (154)\\
&\le H(\mathbf{Y}_i) - H(\mathbf{X}_j) + n\epsilon' + nc && (155)
\end{aligned}$$

for every $i \neq j$, where (155) follows using Lemma 2.

Let Π be any derangement of $(1, \ldots, n)$, and let $j = \Pi(i)$. Then, using (155), we obtain,

$$\sum_{k=1}^{K} H(\mathbf{X}_k) \le \sum_{k=1}^{K} H(\mathbf{Y}_k) - n\sum_{k=1}^{K} R_k + nK(\epsilon' + c) \tag{156}$$

Using (156) in (147), we get,

$$\begin{aligned}
2n\sum_{i=1}^{K} R_i &\le \sum_{k=1}^{K} H(\mathbf{Y}_k) - H(\mathbf{Z}) + nK(\epsilon' + c) + n\epsilon && (157)\\
&\le (K-1)\frac{n}{2}\log P + (H(\mathbf{Y}_K) - H(\mathbf{Z})) + n\epsilon'' && (158)
\end{aligned}$$

where $\epsilon'' = o(\log P)$. Dividing by n and letting $n \to \infty$,

$$\begin{aligned}
2\sum_{i=1}^{K} R_i &\le (K-1)\frac{1}{2}\log P + \epsilon'' \\
&\quad + \lim_{n\to\infty} \frac{1}{n}(H(\mathbf{Y}_K) - H(\mathbf{Z})) && (159)
\end{aligned}$$

Now dividing by $\frac{1}{2}\log P$ and taking $P \to \infty$,

$$\sum_{i=1}^{K} d_i \le \frac{K-1}{2} + \frac{1}{2}\lim_{P\to\infty}\lim_{n\to\infty} \frac{H(\mathbf{Y}_K) - H(\mathbf{Z})}{\frac{n}{2}\log P} \tag{160}$$

3) Bounding the Difference of Entropies: As we did in Section IV-B.3, we enhance the system by relaxing the condition that channel inputs from different transmitters are mutually independent, and think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}_K) - H(\mathbf{Z})$, where $\mathbf{Y}_K$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. Using Lemma 3, the difference of entropies, $H(\mathbf{Y}_K) - H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver is unknown. Thus,

$$H(\mathbf{Y}_K) - H(\mathbf{Z}) \le no(\log P) \tag{161}$$

Using (161) in (160), we have

$$\sum_{i=1}^{K} d_i \le \tfrac{K-1}{2} \tag{162}$$

This completes the converse proof of Theorem 3.

VI. Proof of Theorem 4

As in the previous section, we focus on the fixed channel gains case and defer the achievable scheme for the fading channel gains to Appendix G. Our scheme achieves a sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$, when m of the K transmitters have eavesdropper's CSI for almost all fixed channel gains.

In particular, it achieves the s.d.o.f. tuple $(d_1, \ldots, d_m, d_{m+1}, \ldots, d_K) = \left(\frac{K-1}{m(K-1)+1}, \ldots, \frac{K-1}{m(K-1)+1}, 0, \ldots, 0\right)$. We employ $m(K-1) + K$ mutually independent random variables:

$$\begin{aligned}
&V_{ij}, \quad i = 1, \ldots, m,\ j = 1, \ldots, K,\ j \neq i\\
&U_j, \quad j = 1, \ldots, K
\end{aligned}$$

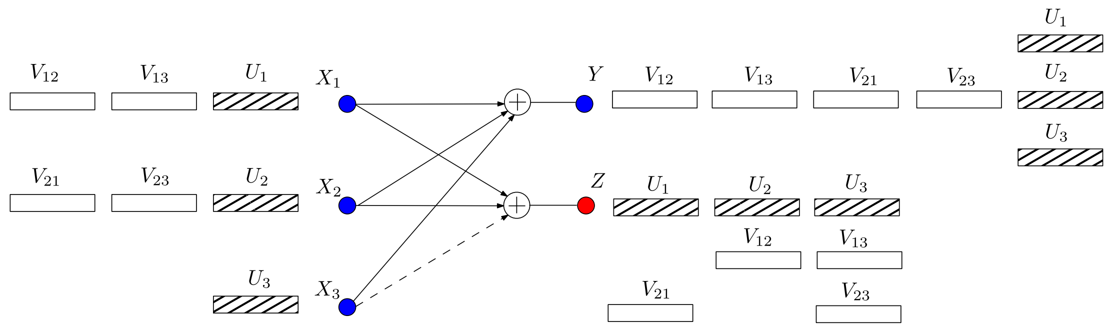

Fig. 6. Alignment of signals when $K = 3$ and $m = 2$.

uniformly drawn from the same PAM constellation $C(a, Q)$ in (21). Transmitter i, $i = 1, \dots, m$ transmits:

$$X_i = \sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j g_i} V_{ij} + \frac{1}{h_i} U_i, \quad i = 1, \dots, m \qquad (163)$$

while transmitters $(m + 1)$ to K transmit

$$X_i = \frac{1}{h_i} U_i, \quad i = m + 1, \dots, K \qquad (164)$$

The channel outputs are given by,

$$Y = \sum_{i=1}^{m} \sum_{j\neq i} \frac{h_i g_j}{h_j g_i} V_{ij} + \sum_{i=1}^{K} U_i + N_1 \qquad (165)$$

$$Z = \sum_{i=1}^{K} \frac{g_i}{h_i} \left(U_i + \sum_{j=1, j\neq i}^{m} V_{ji} \right) + N_2 \qquad (166)$$

Intuitively, every V_{ij} gets superimposed with U_j at the eavesdropper, thus securing it. This is shown in Fig. 6. The proof of decodability and security guarantee follows exactly the proof in [2, Sec. IX-B] and is omitted here.

VII. Conclusions

In this paper, we established the optimal sum s.d.o.f. for three channel models: the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, in the absence of eavesdropper's CSIT. While there is no loss in the s.d.o.f. for the wiretap channel with helpers in the absence of the eavesdropper's CSIT, the s.d.o.f. decreases in the cases of the multiple access wiretap channel and the interference channel with an external eavesdropper. We show that in the absence of eavesdropper's CSIT, the K-user multiple access wiretap channel is equivalent to a wiretap channel with $(K-1)$ helpers from a sum s.d.o.f. perspective. The question of optimality of the sum s.d.o.f. when some but not all of the transmitters have the eavesdropper's CSIT remains a subject of future work.

Appendix A
Achievable Scheme for the Fading Wiretap Channel With Helpers

We present an achievable scheme for the wiretap channel with helpers for the case of fading channel gains, i.e., when the channel gains vary in an i.i.d. fashion from one time slot to another. In this scheme, the legitimate transmitter sends M independent Gaussian symbols, $\mathbf{V} = \{V_2, \dots, V_{M+1}\}$ securely to the legitimate receiver in $(M + 1)$ time slots. This is done as follows:

At time $t = 1, \dots, M + 1$, the legitimate transmitter sends a scaled artificial noise, i.e., cooperative jamming, symbol U_1 along with information symbols as,

$$X_1(t) = \frac{1}{h_1(t)} U_1 + \sum_{k=2}^{M+1} \alpha_k(t) V_k \qquad (167)$$

where the $\alpha_k(t)$s are chosen such that the $(M + 1) \times (M + 1)$ matrix T, with entries $T_{ij} = \alpha_i(j)h_1(j)$, where $\alpha_1(j) = \frac{1}{h_1(j)}$, is full rank. The jth helper, $j = 2, \dots, M + 1$, transmits:

$$X_j(t) = \frac{1}{h_j(t)} U_j \qquad (168)$$

The channel outputs at time t are,

$$Y(t) = \sum_{k=2}^{M+1} h_1(t)\alpha_k(t)V_k + \left(\sum_{j=1}^{M+1} U_j \right) + N_1(t) \qquad (169)$$

$$Z(t) = \sum_{k=2}^{M+1} g_1(t)\alpha_k(t)V_k + \sum_{j=1}^{M+1} \frac{g_j(t)}{h_j(t)} U_j + N_2(t) \qquad (170)$$

Note the similarity of the scheme with that of the real interference scheme for fixed channel gains, i.e., the similarity between (169)-(170) and (24)-(25). Indeed the alignment structure after $(M+1)$ channel uses is exactly as in Fig. 4. Note also how the artificial noise symbols align at the legitimate receiver over $(M + 1)$ time slots. At high SNR, at the end of the $(M + 1)$ slots, the legitimate receiver recovers $(M+1)$ linearly independent equations with $(M+1)$ variables: $V_2, \dots, V_{M+1}, \sum_{j=1}^{M+1} U_j$. Thus, the legitimate receiver can recover $\mathbf{V} \triangleq (V_2, \dots, V_{M+1})$ within noise variance.

Formally, let us define $\mathbf{U} \triangleq (U_1, \dots, U_{M+1})$, $\mathbf{Y} \triangleq (Y(1), \dots, Y(M + 1))$, and $\mathbf{Z} \triangleq (Z(1), \dots, Z(M + 1))$. The observations at the legitimate receiver and the eavesdropper can then be compactly written as

$$\mathbf{Y} = (\mathbf{A}_V, \mathbf{A}_U) \begin{pmatrix} \mathbf{V}^T \\ \mathbf{U}^T \end{pmatrix} + \mathbf{N}_1 \qquad (171)$$

$$\mathbf{Z} = (\mathbf{B}_V, \mathbf{B}_U) \begin{pmatrix} \mathbf{V}^T \\ \mathbf{U}^T \end{pmatrix} + \mathbf{N}_2 \qquad (172)$$

where $\mathbf{A}_V$ is a $(M+1)\times M$ matrix with $(\mathbf{A}_V)_{ij} = h_1(i)\alpha_{j+1}(i)$, $\mathbf{A}_U$ is a $(M+1)\times(M+1)$ matrix with all ones, $\mathbf{B}_V$ is a $(M+1)\times M$ matrix with $(\mathbf{B}_V)_{ij} = g_1(i)\alpha_{j+1}(i)$, and $\mathbf{B}_U$ is a $(M+1)\times(M+1)$ matrix with $(\mathbf{B}_U)_{ij} = \frac{g_j(i)}{h_j(i)}$. $\mathbf{N}_1$ and $\mathbf{N}_2$ are $(M+1)$ dimensional vectors containing the noise variables $N_1(t)$ and $N_2(t)$, respectively, for $t = 1,\ldots,M+1$. To calculate differential entropies, we use the following lemma.

Lemma 4: Let $\mathbf{A}$ *be an* $M\times N$ *dimensional matrix and let* $\mathbf{X} = (X_1,\ldots,X_N)^T$ *be a jointly Gaussian random vector with zero-mean and variance* $P\mathbf{I}$. *Also, let* $\mathbf{N} = (N_1,\ldots,N_M)^T$ *be a jointly Gaussian random vector with zero-mean and variance* $\sigma^2\mathbf{I}$, *independent of* $\mathbf{X}$. *If* $r = rank(\mathbf{A})$, *then,*

$$h(\mathbf{AX}+\mathbf{N}) = r\left(\frac{1}{2}\log P\right) + o(\log P) \tag{173}$$

We present the proof of Lemma 4 in Appendix B.

Using Lemma 4, we compute

$$\begin{aligned}
I(\mathbf{V};\mathbf{Y}) &= h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{V}) && (174)\\
&= (M+1)\frac{1}{2}\log P - h(\mathbf{A}_U\mathbf{U}^T + \mathbf{N}_1) + o(\log P) && (175)\\
&= (M+1)\left(\frac{1}{2}\log P\right) - \frac{1}{2}\log P + o(\log P) && (176)\\
&= M\left(\frac{1}{2}\log P\right) + o(\log P) && (177)
\end{aligned}$$

where (175) follows since $\mathbf{U}$ and $\mathbf{N}_1$ are independent of $\mathbf{V}$ and since $(\mathbf{A}_V, \mathbf{A}_U)$ has rank $(M+1)$ due to the choice of $\alpha_i(t)$s, and (176) follows since $\mathbf{A}_U$ clearly has rank 1. We also have,

$$\begin{aligned}
I(\mathbf{V};\mathbf{Z}) &= h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{V}) && (178)\\
&= (M+1)\frac{1}{2}\log P - h(\mathbf{B}_U\mathbf{U}^T + \mathbf{N}_2) + o(\log P) && (179)\\
&= (M+1)\frac{1}{2}\log P - (M+1)\frac{1}{2}\log P + o(\log P) && (180)\\
&= o(\log P) && (181)
\end{aligned}$$

where we have used the fact that both $(\mathbf{B}_V, \mathbf{B}_U)$ and $\mathbf{B}_U$ have rank $(M+1)$, almost surely, since the $\alpha_i(t)$s do not depend on the $g_i(t)$s and since both the $g_i(t)$s and $h_i(t)$s come from a continuous distribution. Note that, in both calculations above, we have implicitly used the fact that $\mathbf{\Omega}$ is known to both the legitimate receiver and the eavesdropper, and that it appears in the conditioning of each mutual information and differential entropy term. Equation (181) means that the leakage to the eavesdropper does not scale with $\log P$.

Now, consider the vector wiretap channel from $\mathbf{V}$ to $\mathbf{Y}$ and $\mathbf{Z}$, by treating the $M+1$ slots in the scheme above as one channel use. Similar to (26), the following secrecy rate is achievable

$$\begin{aligned}
C_s^{vec} &\geq I(\mathbf{V};\mathbf{Y}) - I(\mathbf{V};\mathbf{Z}) && (182)\\
&= M\left(\frac{1}{2}\log P\right) + o(\log P) && (183)
\end{aligned}$$

Since each channel use of this vector channel uses $(M+1)$ actual channel uses, the achievable rate for the actual channel is,

$$C_s \geq \frac{M}{M+1}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{184}$$

Thus, the achievable s.d.o.f. of this scheme is $\frac{M}{M+1}$. The results in (52) and (184) complete the achievability of Theorem 1, for fixed and fading channel gains, respectively.

Appendix B
Proof of Lemma 4

Since $\mathbf{AX}+\mathbf{N}$ is a jointly Gaussian random vector with zero-mean and covariance $P\mathbf{AA}^T + \sigma^2\mathbf{I}$, we have [33],

$$\begin{aligned}
h(\mathbf{AX}+\mathbf{N}) &= \frac{1}{2}\log(2\pi e)^M\left|P\mathbf{AA}^T + \sigma^2\mathbf{I}\right| && (185)\\
&= \frac{1}{2}\log(2\pi e)^M\left|P\mathbf{W\Sigma W}^T + \sigma^2\mathbf{I}\right| && (186)\\
&= \frac{1}{2}\sum_{i=1}^{r}\log\left(\lambda_i P + \sigma^2\right) + o(\log P) && (187)\\
&= r\left(\frac{1}{2}\log P\right) + o(\log P) && (188)
\end{aligned}$$

where we note that $\mathbf{AA}^T$ is positive semi-definite, with an eigenvalue decomposition $\mathbf{W\Sigma W}^T$, where Σ is a diagonal matrix with r non-zero entries $\lambda_1,\ldots,\lambda_r$.

Appendix C
Proof of Lemma 2

First, note that

$$H(X|\lfloor hX\rfloor, h) = \mathbb{E}_h\left[H(X|\lfloor hX\rfloor, h = \tilde{h})\right] \tag{189}$$

Now, for a fixed h, let us define $S_h(\nu)$ as the set of all realizations of X such that $\lfloor hX\rfloor = \nu$, i.e., $S_h(\nu) \triangleq \left\{i \in \left\{1,\ldots,\lfloor\sqrt{P}\rfloor\right\} : \lfloor ih\rfloor = \nu\right\}$. Then,

$$H\left(X|\lfloor hX\rfloor, h = \tilde{h}\right) \leq \log|S_{\tilde{h}}(\lfloor\tilde{h}X\rfloor)| \tag{190}$$

For any ν, we can upper-bound $|S_{\tilde{h}}(\nu)|$ as follows: Let, i_1 and i_2 be the minimum and maximum elements of $S_{\tilde{h}}(\nu)$. Then, $\lfloor i_1\tilde{h}\rfloor = \lfloor i_2\tilde{h}\rfloor$ implies that $(i_2 - i_1)|\tilde{h}| < 1$, which means $(i_2 - i_1) < \frac{1}{|\tilde{h}|}$. Hence,

$$\begin{aligned}
|S_{\tilde{h}}(\nu)| &\leq i_2 - i_1 + 1 && (191)\\
&< 1 + \frac{1}{|\tilde{h}|} && (192)
\end{aligned}$$

Thus, using (189) and (190), we have,

$$H(X|\lfloor hX\rfloor, h) \leq \mathbb{E}_h\left[\log\left(1 + \frac{1}{|h|}\right)\right] \leq c \tag{193}$$

where c is a constant independent of P.

APPENDIX D
PROOF OF LEMMA 3

Recall that we wish to prove that for the deterministic channel model stated in (53)-(55), with the channel gains to $\mathbf{Z}$ unknown at the transmitter, we have

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \le no(\log P) \tag{194}$$

We first note that we can bound $H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega)$ as:

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \le \sup_{\{\mathbf{X}_i\}:\mathbf{X}_i \perp\!\!\!\perp \mathbf{X}_j} H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \tag{195}$$
$$\le \sup_{\{\mathbf{X}_i\}} H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \tag{196}$$

where $X \perp\!\!\!\perp Y$ is used to denote that X and Y are statistically independent and (196) follows from (195) by relaxing the condition of independence in (195). Since the $\mathbf{X}_i$s in (196) may be arbitrarily correlated, we can think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega)$, where $\mathbf{Y}$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. This brings us to the K-user MISO broadcast channel setting of [9]. The proof then follows by following the steps of [9, eqs. (75)–(103)]; however, we present it here for completeness. The proof has the following steps:

Functional Dependence: For a given channel realization of $\boldsymbol{H} \triangleq \left\{h_i^n, i = 1, \ldots, K\right\}$, there may be multiple vectors $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K)$ that cast the same image at $\boldsymbol{Y}$. Thus, the mapping from $\boldsymbol{Y}, \boldsymbol{H}$ to one of these vectors $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K)$ is random. We denote this map as $\mathcal{L}$, i.e.,

$$(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K) = \mathcal{L}(\boldsymbol{Y}, \boldsymbol{H}) \tag{197}$$

Now, we note that

$$H(\mathbf{Z}|\Omega) \ge H(\mathbf{Z}|\Omega, \mathcal{L}) \tag{198}$$
$$\ge \min_{L \in \{\mathcal{L}\}} H(\mathbf{Z}|\Omega, \mathcal{L} = L) \tag{199}$$

Let the minimizing mapping be L_0. We choose this to be the deterministic mapping

$$(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K) = L_0(\boldsymbol{Y}, \boldsymbol{H}) \tag{200}$$

Essentially, for a given $\boldsymbol{Y}$ and $\boldsymbol{H}$, we choose the mapping that minimizes the entropy at $\mathbf{Z}$. Note that this mapping makes $\boldsymbol{Z}$ a deterministic function of $(\boldsymbol{Y}, \Omega)$, which we denote by $\boldsymbol{Z}(\boldsymbol{Y}, \Omega)$, and that while $H(\boldsymbol{Y}|\Omega)$ is not affected, this choice of $\boldsymbol{Z}$ minimizes $H(\boldsymbol{Z}|\Omega)$, i.e.,

$$H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}|\Omega) \le H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) \tag{201}$$

Further, note that this selection can be done irrespective of any security or decodability constraints.

Aligned Image Sets: For a given channel realization Ω, define the aligned image set $\mathcal{A}(\Omega)$ as the set of all $\boldsymbol{Y}$ that have the same image in $\boldsymbol{Z}$:

$$\mathcal{A}_{\boldsymbol{v}}(\Omega) = \{\boldsymbol{y} : \boldsymbol{Z}(\boldsymbol{y}, \Omega) = \boldsymbol{Z}(\boldsymbol{v}, \Omega)\} \tag{202}$$

Bounding Difference of Entropies via Size of Aligned Sets: We have

$$H(\boldsymbol{Y}|\Omega) = H(\boldsymbol{Y}, \boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) \tag{203}$$
$$= H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + H(\boldsymbol{Y}|\boldsymbol{Z}(\boldsymbol{Y}, \Omega), \Omega) \tag{204}$$
$$= H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + H(\mathcal{A}_{\boldsymbol{Y}}(\Omega)|\Omega) \tag{205}$$
$$\le H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + \mathbb{E}[\log|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] \tag{206}$$
$$\le H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + \log\mathbb{E}[|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] \tag{207}$$

Therefore, we have,

$$H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) \le \mathbb{E}[|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] \tag{208}$$

Bounding the Probability of Alignment: Given the channel $\boldsymbol{H}$ and two realizations $\boldsymbol{y}$ and $\boldsymbol{y}'$ of $\boldsymbol{Y}$, such that $\boldsymbol{X}_j(\boldsymbol{y}, \boldsymbol{H}) = \boldsymbol{x}_j$, and $\boldsymbol{X}'_j(\boldsymbol{y}', \boldsymbol{H}) = \boldsymbol{x}'_j$, we bound the probability of image alignment at $\boldsymbol{Z}$. Note that for alignment, we must have for all $t = 1, \ldots, n$,

$$\sum_{i=1}^{K} \lfloor g_i(t) x_i(t) \rfloor = \sum_{i=1}^{K} \left\lfloor g_i(t) x_i'(t) \right\rfloor \tag{209}$$

which implies

$$g_{i^*(t)}(t)(x'_{i^*}(t) - x_{i^*}(t)) \in \sum_{i=1, i \ne i^*(t)}^{K} \lfloor g_i(t) x_i(t) \rfloor - \left\lfloor g_i(t) x_i'(t) \right\rfloor + \Delta \tag{210}$$

where $\Delta \in (-1, 1)$, and

$$i^*(t) = \arg\max_i |(x_i'(t) - x_i(t)| \tag{211}$$

Therefore, for any t such that $x'_{i^*}(t) \ne x_{i^*}(t)$, $g_{i^*(t)}(t)$ must lie within an interval of length $\frac{2}{|x'_{i^*}(t) - x_{i^*}(t)|}$. If $f_{\max}$ is the maximum of 1 and an upper bound on the probability density function of $g_i(t)$ (note that the probability density is assumed to be bounded), we have,

$$\mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \le f_{\max}^n \prod_{\substack{t: x'_{i^*(t)}(t) \\ \ne \\ x_{i^*(t)}(t)}} \frac{2}{|x'_{i^*(t)}(t) - x_{i^*(t)}(t)|} \tag{212}$$

We now express this probability in terms of $y(t)$ and $y'(t)$ as follows: We note

$$y'(t) - y(t) = \sum_{i=1}^{K} \left(\lfloor h_i(t) x_i(t) \rfloor - \left\lfloor h_i(t) x_i'(t) \right\rfloor\right) \tag{213}$$
$$\le \sum_{i=1}^{K} \left\lfloor h_i(t)(x_i(t) - x'(t)) \right\rfloor + (-K, K) \tag{214}$$

Therefore, we have

$$|y'(t) - y(t)| \le |x'_{i^*(t)}(t) - x_{i^*(t)}(t)| \sum_{i=1}^{K} |h_i(t)| + K \tag{215}$$

which implies

$$\frac{1}{|x'_{i^*(t)}(t) - x_{i^*(t)}(t)|} \le \frac{\sum_{i=1}^{K} |h_i(t)|}{|y'(t) - y(t)| - K} \tag{216}$$

whenever $|y'(t) - y(t)| > K$. Thus, we have

$$\mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \leq \bar{h}^n f_{\max}^n \prod_{t:|y'(t)-y(t)|>K} \frac{1}{|y'(t) - y(t)| - K} \tag{217}$$

where

$$\bar{h}^n = \max\left(1, \prod_{t:x'_{i^*(t)}(t)\neq x_{i^*(t)}(t)} 2\sum_{i=1}^{K} |h_i(t)|\right) \tag{218}$$

Bounding the Size of the Aligned Image Set:

$$\mathbb{E}[|\mathcal{A}_{\boldsymbol{y}}(\Omega)|] = \sum_{\boldsymbol{y}'} \mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \tag{219}$$

$$\leq \bar{h}^n f_{\max}^n \prod_{t=1}^{n} \left(\sum_{y'(t):|y'(t)-y(t)|\leq K} 1 + \sum_{y'(t):K<|y'(t)-y(t)|\leq Q_y(t)} \frac{1}{|y'(t) - y(t)| - K} \right) \tag{220}$$

$$\leq \bar{h}^n f_{\max}^n \left(\log \sqrt{P} + o(\log P)\right)^n \tag{221}$$

where $Q_y(t) \leq \sqrt{P}\sum_{i=1}^{K} |h_i(t)| + K$. Therefore, taking logarithms, we have

$$\log \mathbb{E}[|\mathcal{A}_{\boldsymbol{y}}(\Omega)|] \leq no(\log P) \tag{222}$$

Now, combining (201), (208) and (222), we have the desired result, i.e.,

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq no(\log P) \tag{223}$$

which completes the proof of Lemma 3.

APPENDIX E
ACHIEVABILITY FOR $K = 3$ WITH FADING CHANNEL GAINS

Our scheme uses asymptotic vector space alignment introduced in [7]. Let $\Gamma = (K-1)^2 = (3-1)^2 = 4$. We use $M_n = 2n^\Gamma + 4(n+1)^\Gamma$ channel uses to transmit $6n^\Gamma$ message symbols securely to the legitimate receivers in the presence of the eavesdropper. Thus, we achieve a sum s.d.o.f. of $\frac{6n^\Gamma}{2n^\Gamma+4(n+1)^\Gamma}$, which approaches 1 as $n \to \infty$.

First, at transmitter i, we divide its message W_i into 2 sub-messages V_{ij}, $j = 1, \ldots, 4$, $j \neq i, i+1$. Each V_{ij} is encoded into n^Γ independent streams $v_{ij}(1), \ldots, v_{ij}(n^\Gamma)$, which we denote as $\mathbf{v}_{ij} \triangleq \left(v_{ij}(1), \ldots, v_{ij}(n^\Gamma)\right)^T$. We also require artificial noise symbols U_i and $\tilde{U}_i$ at each transmitter i. We encode the artificial noise symbols U_i and $\tilde{U}_i$ as

$$\mathbf{u}_i \triangleq \left(u_i(1), \ldots, u_i((n+1)^\Gamma)\right)^T, i = 1, 2, 3 \tag{224}$$

$$\tilde{\mathbf{u}}_i \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i(n^\Gamma)\right)^T, i = 1, 2 \tag{225}$$

$$\tilde{\mathbf{u}}_3 \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i((n+1)^\Gamma)\right)^T \tag{226}$$

In each channel use $t \leq M_n$, we choose precoding column vectors $\mathbf{p}_{ij}(t)$, $\mathbf{q}_i(t)$ and $\tilde{\mathbf{q}}_i(t)$ with the same number of elements as $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. In channel use t, transmitter i sends

$$X_i(t) = \sum_{j\neq i,i+1} \mathbf{p}_{ij}(t)^T \mathbf{v}_{ij} + \mathbf{q}_i(t)^T \mathbf{u}_i + \tilde{\mathbf{q}}_i(t)^T \tilde{\mathbf{u}}_i \tag{227}$$

where we have dropped the limits on j in the summation for notational simplicity. By stacking the precoding vectors for all M_n channel uses, we let,

$$\mathbf{P}_{ij} = \begin{pmatrix} \mathbf{p}_{ij}(1)^T \\ \vdots \\ \mathbf{p}_{ij}^T(M_n) \end{pmatrix}, \quad \mathbf{Q}_i = \begin{pmatrix} \mathbf{q}_i(1)^T \\ \vdots \\ \mathbf{q}_i(M_n)^T \end{pmatrix} \tag{228}$$

and,

$$\tilde{\mathbf{Q}}_i = \begin{pmatrix} \tilde{\mathbf{q}}_i(1)^T \\ \vdots \\ \tilde{\mathbf{q}}_i(M_n)^T \end{pmatrix} \tag{229}$$

Now, letting $\mathbf{X}_i = (X_i(1), \ldots, X_i(M_n))^T$, the channel input for transmitter i over M_n channel uses can be compactly represented as

$$\mathbf{X}_i = \sum_j \mathbf{P}_{ij}\mathbf{v}_{ij} + \mathbf{Q}_i\mathbf{u}_i + \tilde{\mathbf{Q}}_i\tilde{\mathbf{u}}_i \tag{230}$$

Recall that, channel use t, the channel output at receiver l and the eavesdropper are, respectively, given by

$$Y_l(t) = \sum_{k=1}^{3} h_{kl}(t)X_k(t) + N_l(t) \tag{231}$$

$$Z(t) = \sum_{k=1}^{3} g_k(t)X_k(t) + N_Z(t) \tag{232}$$

Let $\mathbf{H}_{kl} \triangleq \text{diag}\,(h_{kl}(1), \ldots, h_{kl}(M_n))$. Similarly, define $\mathbf{G}_k = \text{diag}\,(g_k(1), \ldots, g_k(M_n))$. The channel outputs at receiver l and the eavesdropper over all M_n channel uses, $\mathbf{Y}_l = (Y_l(1), \ldots, Y_l(M_n))^T$ and $\mathbf{Z} = (Z(1), \ldots, Z(M_n))^T$, respectively, can be represented by

$$\mathbf{Y}_l = \sum_{k=1}^{3} \mathbf{H}_{kl}\mathbf{X}_k + \mathbf{N}_l \tag{233}$$

$$= \sum_{k=1}^{3} \mathbf{H}_{kl} \left(\sum_{\substack{j=1 \\ j\neq k,k+1}}^{4} \mathbf{P}_{kj}\mathbf{v}_{kj} + \mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k \right) + \mathbf{N}_l \tag{234}$$

$$= \sum_{\substack{j=1 \\ j\neq l,l+1}}^{4} \mathbf{H}_{ll}\mathbf{P}_{lj}\mathbf{v}_{lj} + \sum_{\substack{k=1 \\ k\neq l}}^{3} \sum_{\substack{j=1 \\ j\neq k,k+1}}^{4} \mathbf{H}_{kl}\mathbf{P}_{kj}\mathbf{v}_{kj} + \sum_{k=1}^{3} \mathbf{H}_{kl}\left(\mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_l \tag{235}$$

TABLE II
SUMMARY OF ALIGNMENT EQUATIONS

	$\mathbf{Q}_1$	$\mathbf{Q}_2$	$\mathbf{Q}_3$	$\tilde{\mathbf{Q}}_3$
Receiver 1	$\mathbf{H}_{21}\mathbf{P}_{21} \preceq \mathbf{H}_{11}\mathbf{Q}_1$ $\mathbf{H}_{31}\mathbf{P}_{31} \preceq \mathbf{H}_{11}\mathbf{Q}_1$	$\mathbf{H}_{11}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{21}\mathbf{Q}_2$ $\mathbf{H}_{31}\mathbf{P}_{32} \preceq \mathbf{H}_{21}\mathbf{Q}_2$	$\mathbf{H}_{21}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{31}\mathbf{Q}_3$	$\mathbf{H}_{21}\mathbf{P}_{24} \preceq \mathbf{H}_{31}\tilde{\mathbf{Q}}_3$
Receiver 2	$\mathbf{H}_{32}\mathbf{P}_{31} \preceq \mathbf{H}_{12}\mathbf{Q}_1$	$\mathbf{H}_{12}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{22}\mathbf{Q}_2$ $\mathbf{H}_{32}\mathbf{P}_{32} \preceq \mathbf{H}_{22}\mathbf{Q}_2$	$\mathbf{H}_{22}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{32}\mathbf{Q}_3$ $\mathbf{H}_{12}\mathbf{P}_{13} \preceq \mathbf{H}_{32}\mathbf{Q}_3$	$\mathbf{H}_{12}\mathbf{P}_{14} \preceq \mathbf{H}_{32}\tilde{\mathbf{Q}}_3$
Receiver 3	$\mathbf{H}_{23}\mathbf{P}_{21} \preceq \mathbf{H}_{13}\mathbf{Q}_1$	$\mathbf{H}_{13}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{23}\mathbf{Q}_2$	$\mathbf{H}_{23}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{33}\mathbf{Q}_3$ $\mathbf{H}_{13}\mathbf{P}_{13} \preceq \mathbf{H}_{33}\mathbf{Q}_3$	$\mathbf{H}_{23}\mathbf{P}_{24} \preceq \mathbf{H}_{33}\tilde{\mathbf{Q}}_3$ $\mathbf{H}_{13}\mathbf{P}_{14} \preceq \mathbf{H}_{33}\tilde{\mathbf{Q}}_3$

TABLE III
VALUES OF T_{ij}

	T_{1j}	T_{2j}	T_{3j}	T_{4j}
$j=1$	$\mathbf{H}_{11}^{-1}\mathbf{H}_{21}$	$\mathbf{H}_{21}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{31}^{-1}\mathbf{H}_{21}\mathbf{H}_{22}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{31}^{-1}\mathbf{H}_{21}$
$j=2$	$\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{22}^{-1}\mathbf{H}_{12}\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{32}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{32}^{-1}\mathbf{H}_{12}$
$j=3$	$\mathbf{H}_{12}^{-1}\mathbf{H}_{32}$	$\mathbf{H}_{22}^{-1}\mathbf{H}_{32}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{23}\mathbf{H}_{22}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{23}$
$j=4$	$\mathbf{H}_{13}^{-1}\mathbf{H}_{23}$	$\mathbf{H}_{23}^{-1}\mathbf{H}_{13}\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{13}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{13}$

and,

$$\mathbf{Z} = \sum_{k=1}^{3} \mathbf{G}_k\mathbf{X}_k + \mathbf{N}_Z \tag{236}$$

$$= \sum_{k=1}^{3} \sum_{\substack{j=1 \\ j\neq k,k+1}}^{4} \mathbf{G}_k\mathbf{P}_{kj}\mathbf{v}_{kj} + \sum_{k=1}^{3} \mathbf{G}_k\left(\mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_Z \tag{237}$$

Now, receiver l wants to decode $\mathbf{v}_{lj}$, $j = 1, \ldots, 4$, $j \neq l$, $l+1$. Thus, the remaining terms in (235) constitute interference at the lth receiver. Let $CS(\mathbf{X})$ denote the column space of matrix $\mathbf{X}$. Then, I_l denoting the space spanned by this interference is given by

$$I_l = \left(\bigcup_{k\neq l, j\neq k,k+1} CS\left(\mathbf{H}_{kl}\mathbf{P}_{kj}\right)\right) \bigcup \left(\bigcup_{k=1}^{3} CS\left(\mathbf{H}_{kl}\mathbf{Q}_k\right)\right) \bigcup \left(\bigcup_{k=1}^{3} CS\left(\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k\right)\right) \tag{238}$$

Note that there are $2n^\Gamma$ symbols to be decoded by each legitimate receiver in $2n^\Gamma + 4(n+1)^\Gamma$ channel uses. Thus, for decodability, the interference can occupy a subspace of rank at most $4(n+1)^\Gamma$, that is,

$$\text{rank}(I_l) \leq 4(n+1)^\Gamma \tag{239}$$

To that end, we align the noise and message subspaces at each legitimate receiver appropriately. Note that no such alignment is possible at the external eavesdropper since the transmitters do not have its CSI. In addition, note that we have a total of $2n^\Gamma + 4(n+1)^\Gamma$ artificial noise symbols which will span the full received signal space at the eavesdropper and secure all the messages.

Fig. 5 shows the alignment we desire. We remark that the same figure represents the alignment of signals both for real interference alignment and the vector space alignment schemes. Now, let us enumerate the conditions for the desired signal alignment at each receiver. From Fig. 5, it is clear that there are 6 alignment equations at each legitimate receiver, corresponding to four unintended messages and two artificial noise symbols $\tilde{U}_1$ and $\tilde{U}_2$. Table II shows the alignment equations for each legitimate receiver.

Now, me make the following selections:

$$\mathbf{P}_{21} = \mathbf{P}_{31} \stackrel{\Delta}{=} \tilde{\mathbf{P}}_1 \tag{240}$$

$$\mathbf{P}_{32} \stackrel{\Delta}{=} \tilde{\mathbf{P}}_2 \tag{241}$$

$$\mathbf{P}_{13} \stackrel{\Delta}{=} \tilde{\mathbf{P}}_3 \tag{242}$$

$$\mathbf{P}_{14} = \mathbf{P}_{24} \stackrel{\Delta}{=} \tilde{\mathbf{P}}_4 \tag{243}$$

$$\tilde{\mathbf{Q}}_1 = \mathbf{H}_{11}^{-1}\mathbf{H}_{31}\tilde{\mathbf{P}}_2 \tag{244}$$

$$\tilde{\mathbf{Q}}_2 = \mathbf{H}_{22}^{-1}\mathbf{H}_{12}\tilde{\mathbf{P}}_3 \tag{245}$$

Note that (244) and (245) imply that the artificial noises $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ align exactly with unintended message symbols $\mathbf{v}_{32}$ and $\mathbf{v}_{13}$ at receivers 1 and 2, respectively. With these selections, it suffices to find matrices $\tilde{\mathbf{P}}_i, i = 1, \ldots, 4$, $\mathbf{Q}_i, i = 1, 2, 3$, and $\tilde{\mathbf{Q}}_3$. The alignment equations may now be written as

$$\mathbf{T}_{ij}\tilde{\mathbf{P}}_i \preceq \mathbf{Q}_i, \quad i = 1, 2, 3, \quad j = 1, \ldots, 4 \tag{246}$$

$$\mathbf{T}_{4j}\tilde{\mathbf{P}}_4 \preceq \tilde{\mathbf{Q}}_3, \quad j = 1, \ldots, 4 \tag{247}$$

where the T_{ij}s are tabulated in Table III, and the notation $\mathbf{A} \preceq \mathbf{B}$ is used to denote that $CS(\mathbf{A}) \subseteq CS(\mathbf{B})$ for matrices $\mathbf{A}$ and $\mathbf{B}$ where $CS(\mathbf{X})$ refers to the column space of the matrix $\mathbf{X}$.

We can now construct the matrices $\tilde{\mathbf{P}}_i, i = 1, \ldots, 4$, $\mathbf{Q}_i, i = 1, \ldots, 3$ and $\tilde{\mathbf{Q}}_3$ as in [7]

$$\tilde{\mathbf{P}}_i = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_i : \alpha_j \in \{1, \ldots, n\} \right\} \tag{248}$$

$$\mathbf{Q}_i = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_i : \alpha_j \in \{1, \ldots, n+1\} \right\} \tag{249}$$

$$\tilde{\mathbf{Q}}_3 = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_4 : \alpha_j \in \{1, \ldots, n+1\} \right\} \tag{250}$$

where each $\mathbf{w}_i$ is the $M_n \times 1$ column vector containing elements drawn independently from a continuous distribution with bounded support. Note that an element in $\mathbf{P}_i$ is the product of powers of some channel coefficients and an extra random variable, just like an element in the sets T_i defined for the real interference scheme. Further, the set of channel coefficients appearing in $\mathbf{P}_i$ is the same as those contained in set T_i. Thus, there is a loose correspondence between the real and vector space alignment techniques.

Now, consider the decodability of the desired signals at the receivers. For example, consider receiver 1. Due to the alignment conditions in Table II, the interference subspace at receiver 1 is given by

$$\mathbf{I}_1 = \left[\mathbf{H}_{11}\mathbf{Q}_1 \quad \mathbf{H}_{21}\mathbf{Q}_2 \quad \mathbf{H}_{31}\mathbf{Q}_3 \quad \mathbf{H_{31}}\tilde{\mathbf{Q}}_3 \right] \tag{251}$$

The desired signal subspace, on the other hand, is

$$\mathbf{D}_1 = \left[\mathbf{H}_{11}\tilde{\mathbf{P}}_3 \quad \mathbf{H}_{11}\tilde{\mathbf{P}}_4 \right] \tag{252}$$

For decodability, it suffices to show that

$$\Lambda_1 = [\mathbf{D}_1 \quad \mathbf{I}_1] \tag{253}$$

is full rank. To do so, we use [34, Lemmas 1 and 2]. Consider any row m of the matrix Λ_1. Note that the mth row of $\mathbf{H}_{i1}\mathbf{Q}_i$ contains the term w_{mi} with exponent 1, but no w_{mj} for $i \neq j$, where w_{mi} denotes the element in the mth row of $\mathbf{w}_i$. In fact, for $i = 1, \ldots, 4$, the term w_{mi} occurs nowhere else in the matrix Λ_l except in $\mathbf{H}_{i1}\mathbf{Q}_i$ ($\mathbf{H}_{31}\tilde{\mathbf{Q}}_3$, when $i = 4$) and $\mathbf{H}_{11}\tilde{\mathbf{P}}_i$. This shows that $\mathbf{D}_1$ and $\mathbf{I}_1$ have full column ranks individually. Further, the matrix $\left[\mathbf{H}_{11}\tilde{\mathbf{P}}_3 \quad \mathbf{H}_{31}\mathbf{Q}_3 \right]$ has full column rank because $\mathbf{Q}_3$ does not contain any elements of $\mathbf{H}_{11}$. Similarly, $\left[\mathbf{H}_{11}\tilde{\mathbf{P}}_4 \quad \mathbf{H}_{31}\tilde{\mathbf{Q}}_3 \right]$ is full column rank for the same reason. Thus, Λ_1, which is a $M_n \times M_n$ matrix, is full column rank, and hence full rank. This ensures decodability of the desired signals at receiver 1. a similar analysis holds for the other receivers as well.

The security of the message signals at the eavesdropper is ensured by the fact that the artificial noises $\mathbf{Q}_i$ and $\tilde{\mathbf{Q}}_i$, $i = 1, 2, 3$, do not align at the eavesdropper, and instead span the full received signal space at the eavesdropper. Indeed, the $M_n \times M_n$ matrix

$$\mathbf{I}_E = \left[\mathbf{G}_1\mathbf{Q}_1 \quad \mathbf{G}_2\mathbf{Q}_2 \quad \mathbf{G}_3\mathbf{Q}_3 \quad \mathbf{G}_1\tilde{\mathbf{Q}}_1 \quad \mathbf{G}_2\tilde{\mathbf{Q}}_2 \quad \mathbf{G}_3\tilde{\mathbf{Q}}_3 \right] \tag{254}$$

is full rank. Thus, if $\mathbf{V}_i = \{\mathbf{v}_{ij}, j \neq i, i+1\}$ denotes the collection of all messages of transmitter i, and $\mathbf{u}^T = \left[\mathbf{u}_1^T, \mathbf{u}_2^T, \mathbf{u}_2^T, \tilde{\mathbf{u}}_1^T, \tilde{\mathbf{u}}_2^T, \tilde{\mathbf{u}}_3^T \right]$,

$$\begin{aligned} I(\mathbf{V}_1^3; \mathbf{Z}) &= h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{V}_1^3) && (255)\\ &= h(\mathbf{Z}) - h(\mathbf{I}_E\mathbf{u}) && (256)\\ &\leq \frac{M_n}{2}\log P - \frac{M_n}{2}\log P + o(\log P) && (257)\\ &= o(\log P) && (258) \end{aligned}$$

In the above calculation, we have dropped the conditioning on $\mathbf{\Omega}$ for notational simplicity. Now, by treating all M_n channel uses as 1 vector channel use, and using [4, Th. 2], an achievable rate for the vector channel is

$$\begin{aligned} R_i^{M_n} &= I(\mathbf{V}_i; \mathbf{Y}_i) - I(\mathbf{V}_i; \mathbf{Z}|\mathbf{V}_{-i}) && (259)\\ &= \quad 2n^\Gamma \log P - o(\log P) && (260) \end{aligned}$$

where (260) follows since the $2n^\Gamma$ symbols are decodable within noise variance, and since $I(\mathbf{V}_i; \mathbf{Z}|\mathbf{V}_{-i}) \leq I(\mathbf{V}_1^3; \mathbf{Z}) \leq o(\log P)$. Thus, the rate $\frac{2n^\Gamma}{M_n}$ is achievable per user pair per channel use, which gives a sum s.d.o.f. of $\frac{6n^\Gamma}{2n^\Gamma+4(n+1)^\Gamma}$, which approaches 1, as $n \to \infty$.

Appendix F
Achievability for the K-User Interference Channel With an External Eavesdropper

Here, we present the general achievable schemes for the K-user interference channel with an external eavesdropper.

A. Fixed Channel Gains

Let m be a large constant. We pick $(K + 1)$ points $c_1, \ldots, c_{K+1}$ in an i.i.d. fashion from a continuous distribution with bounded support. Then, $c_1, \ldots, c_{K+1}$ are rationally independent almost surely. Let us define sets T_i, for $i = 1, \ldots, K + 1$, which will represent *dimensions* as follows:

$$T_1 \triangleq \left\{ \left(\prod_{k=1}^{K} h_{1k}^{r_{1k}} \right) \left(\prod_{j,k=1, j\neq 1,k}^{K} h_{jk}^{r_{jk}} \right) c_1^s : r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{261}$$

$$T_i \triangleq \left\{ \left(\prod_{k=1}^{K} h_{ik}^{r_{ik}} \right) \left(\prod_{k=2}^{K} \left(\frac{h_{(i-1)k}}{h_{(i-1)1}} \right)^{r_{(i-1)k}} \right) \left(\prod_{\substack{j,k=1\\ j\neq i,i-1,k}}^{K} h_{jk}^{r_{jk}} \right) c_i^s : r_{jk}, s \in \{1, \ldots, m\} \right\}, \quad i = 2, \ldots, K-1 \tag{262}$$

$$T_K \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{k=1,k\neq 2}^{K} \left(\frac{h_{(K-1)k}}{h_{(K-1)2}} \right)^{r_{(K-1)k}} \right) \left(\prod_{\substack{j,k=1\\ j\neq K,K-1,k}}^{K} h_{jk}^{r_{jk}} \right) c_K^s : r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{263}$$

$$T_{K+1} \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{j,k=1, j \neq K,k}^{K} h_{jk}^{r_{jk}} \right) c_{K+1}^{s} : r_{jk}, s \in \{1, \ldots, m\} \right\} \quad (264)$$

Let M_i be the cardinality of T_i. Note that all M_i are the same, thus we denote them as M,

$$M \triangleq m^{2+K(K-1)} \quad (265)$$

First, we divide each message into many sub-messages; specifically, the message of the ith transmitter, W_i, is divided into $(K-1)$ sub-messages V_{ij}, $j = 1, \ldots, K+1$, $j \neq i, i+1$. For each transmitter i, let $\mathbf{p}_{ij}$ be the vector containing all the elements of T_j, for $j \neq i, i+1$. For any given (i, j) with $j \neq i, i+1$, $\mathbf{p}_{ij}$ represents the dimension along which message V_{ij} is sent. Further, at each transmitter i, let $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ be vectors containing all the elements in sets T_i and $\beta_i T_{i+1}$, respectively, where

$$\beta_i = \begin{cases} \frac{h_{(i+2)1}}{h_{i1}}, & \text{if } 1 \leq i \leq K-2 \\ \frac{h_{12}}{h_{i2}}, & \text{if } i = K-1 \\ 1, & \text{if } i = K \end{cases} \quad (266)$$

The vectors $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ represent dimensions along which artificial noise symbols U_i and $\tilde{U}_i$, respectively, are sent. We define a $(K+1)M$ dimensional vector $\mathbf{b}_i$ by stacking the $\mathbf{p}_{ij}$s, $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ as

$$\mathbf{b}_i^T = \left[\mathbf{p}_{i1}^T \ldots \mathbf{p}_{i(i-1)}^T \quad \mathbf{p}_{i(i+2)}^T \ldots \mathbf{p}_{i(K+1)} \quad \mathbf{q}_i \quad \tilde{\mathbf{q}}_i \right] \quad (267)$$

The transmitter encodes V_{ij} using an M dimensional vector $\mathbf{v}_{ij}$, and the cooperative jamming signals U_i and $\tilde{U}_i$ using M dimensional vectors $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. Each element of $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$ are drawn in an i.i.d. fashion from $C(a, Q)$ in (21). Let

$$\mathbf{a}_i^T = \left[\mathbf{v}_{i1}^T \ldots \mathbf{v}_{i(i-1)}^T \quad \mathbf{v}_{i(i+2)}^T \ldots \mathbf{v}_{i(K+1)} \quad \mathbf{u}_i \quad \tilde{\mathbf{u}}_i \right] \quad (268)$$

The channel input of transmitter i is then given by

$$x_i = \mathbf{a}_i^T \mathbf{b} \quad (269)$$

Let us now analyze the structure of the received signals at the legitimate receivers. The alignment of the interfering signal spaces at receiver i is shown in Fig. 7. The ith row depicts the signals originating from transmitter i. The signals in the same column align together at the receiver. For simplicity of exposition, let us consider receiver 1.

At the first receiver, the desired signals $\mathbf{v}_{13}, \ldots, \mathbf{v}_{1(K+1)}$ come along dimensions $h_{11}T_3, \ldots, h_{11}T_{K+1}$, respectively. These dimensions are *separate* almost surely, since T_i contains powers of c_i while T_j, $j \neq i$ does not. Thus, they correspond to *separate* boxes in the Fig. 5 for $K = 3$. For the same reason, cooperative jamming signals $\mathbf{u}_1, \ldots, \mathbf{u}_K$, $\tilde{\mathbf{u}}_K$, which arrive along the dimensions $h_{11}T_1, \ldots, h_{K1}T_K$, $h_{K1}T_{K+1}$ occupy different dimensions almost surely. Further, the message signals $\mathbf{v}_{13}, \ldots, \mathbf{v}_{1(K+1)}$, and the cooperative jamming signals $\mathbf{u}_1, \ldots, \mathbf{u}_K, \tilde{\mathbf{u}}_K$ do not overlap, since none of $T_3 \ldots, T_{K+1}$ contain h_{11}. Thus, they appear as separate boxes in Fig. 5.

Now, let us consider the signals that are not desired at receiver 1. A signal $\mathbf{v}_{kl}$, $k \neq 1, K+1$ arrives at receiver 1 along $h_{k1}T_l$. If we define

$$\tilde{T}_1 \triangleq \left\{ \left(\prod_{k=1}^{K} h_{1k}^{r_{1k}} \right) \left(\prod_{j,k=1, j \neq 1,k}^{K} h_{jk}^{r_{jk}} \right) c_1^s : r_{jk}, s \in \{1, \ldots, m+1\} \right\} \quad (270)$$

$$\tilde{T}_i \triangleq \left\{ \left(\prod_{k=1}^{K} h_{ik}^{r_{ik}} \right) \left(\prod_{k=2}^{K} \left(\frac{h_{(i-1)k}}{h_{(i-1)1}} \right)^{r_{(i-1)k}} \right) \left(\prod_{\substack{j,k=1 \\ j \neq i, i-1, k}}^{K} h_{jk}^{r_{jk}} \right) c_i^s : r_{jk}, s \in \{1, \ldots, m+1\} \right\},$$
$$i = 2, \ldots, K-1 \quad (271)$$

$$\tilde{T}_K \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{\substack{k=1, k \neq 2 \\ m=K-1}}^{K} \left(\frac{h_{mk}}{h_{m2}} \right)^{r_{mk}} \right) \left(\prod_{\substack{j,k=1 \\ j \neq K, K-1, k}}^{K} h_{jk}^{r_{jk}} \right) c_K^s : r_{jk}, s \in \{1, \ldots, m+1\} \right\} \quad (272)$$

$$\tilde{T}_{K+1} \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{j,k=1, j \neq K,k}^{K} h_{jk}^{r_{jk}} \right) c_{K+1}^{s} : r_{jk}, s \in \{1, \ldots, m+1\} \right\} \quad (273)$$

we notice that the dimensions in $h_{k1}T_l$, $k \neq 1$ are subsets of $\tilde{T}_l$, as is $h_{l1}T_l$ for every $l = 1, \ldots, K$. Thus, each $\mathbf{v}_{kl}$ aligns with $\mathbf{u}_l$ in $\tilde{T}_l$, for $l = 1, \ldots, K$, as is shown in Fig. 7. Further, a signal $\mathbf{v}_{k(K+1)}$, $k \neq 1, K$, arrives along the dimensions $h_{k1}T_{K+1}$, $k \neq 1$ which is a subset of $\tilde{T}_{K+1}$, as is $h_{K1}T_{K+1}$, along which $\tilde{\mathbf{u}}_K$ arrives. Thus, each $\mathbf{v}_{k(K+1)}$, $k \neq 1, K$ aligns with $\tilde{\mathbf{u}}_K$, see Fig. 7. Finally, the cooperative jamming signals $\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_{K-2}$, and $\tilde{\mathbf{u}}_{K-1}$ arrive at receiver 1 along dimensions $h_{31}T_2, \ldots, h_{K1}T_{K-1}$, and $h_{12}\left(\frac{h_{(K-1)1}}{h_{(K-1)2}}\right)T_K$, respectively, which are all in $\tilde{T}_2 \ldots, \tilde{T}_{K-1}$ and $\tilde{T}_K$, respectively. Thus, the signal $\tilde{\mathbf{u}}_i$, $i = 1, \ldots, K-1$ align with $\mathbf{u}_{i+1}$ in $\tilde{T}_{i+1}$, which is seen in Fig. 5 for $K = 3$, and in Fig. 7 for general K.

We further note that the sets $h_{11}T_3, \ldots, h_{11}T_{K+1}, \tilde{T}_1, \ldots, \tilde{T}_{K+1}$ are all separable since only T_i and $\tilde{T}_i$ (and not T_j or $\tilde{T}_j$) contain powers of c_i, and none of $\tilde{T}_3, \ldots, \tilde{T}_{K+1}$ contains h_{11}. A similar observation holds for the received signal at any of the remaining receivers. Thus, the set

$$S = \left(\bigcup_{i=3}^{K+1} h_{11} T_i \right) \bigcup \left(\bigcup_{i=1}^{K+1} \tilde{T}_i \right) \quad (274)$$

	T_1	T_2	T_3	T_4	$\bullet\bullet\bullet$	T_{j-1}	T_j	T_{j+1}	T_{j+2}	$\bullet\bullet\bullet$	T_i	T_{i+1}		T_{K+1}
Tx 1	U_1	$\tilde{U}_1$	V_{13}	V_{14}	$\bullet\bullet\bullet$	$V_{1(j-1)}$	V_{1j}	$V_{1(j+1)}$	$V_{1(j+2)}$	$\bullet\bullet\bullet$	V_{1i}	$V_{1(i+1)}$	$\bullet\bullet\bullet$	V_{1K}
Tx 2	V_{21}	U_2	$\tilde{U}_2$	V_{24}	$\bullet\bullet\bullet$	$V_{2(j-1)}$	V_{2j}	$V_{2(j+1)}$	$V_{2(j+2)}$	$\bullet\bullet\bullet$	V_{2i}	$V_{2(i+1)}$	$\bullet\bullet\bullet$	V_{2K}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Tx j	V_{j1}	V_{j2}	V_{j3}	V_{j4}	$\bullet\bullet\bullet$	$V_{j(j-1)}$	U_j	$\tilde{U}_j$	$V_{j(j+2)}$	$\bullet\bullet\bullet$	V_{ji}	$V_{j(i+1)}$	$\bullet\bullet\bullet$	V_{jK}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Tx i											U_i	$\tilde{U}_i$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Tx K	V_{K1}	V_{K2}	V_{K3}	V_{K4}	$\bullet\bullet\bullet$	$V_{K(j-1)}$	V_{Kj}	$V_{K(j+1)}$	$V_{K(j+2)}$	$\bullet\bullet\bullet$	V_{Ki}	$V_{K(i+1)}$	$\bullet\bullet\bullet$	$\tilde{U}_K$

Fig. 7. Alignment of interference signals at receiver i.

has cardinality given by

$$M_s = (K-1)m^{K(K-1)+2} + (K+1)(m+1)^{K(K-1)+2} \tag{275}$$

At the external eavesdropper, there is no alignment and the cooperative jamming signals occupy the full space, thereby exhausting the decoding capability of the eavesdropper. This secures all the messages at the external eavesdropper.

We next provide an analysis for the achievable sum rate. Since we have only one eavesdropper, we use [4, Th. 2] and observe that the rate

$$R_i = I(V_i; Y_i) - I(V_i; Z|V_{-i}) \tag{276}$$

is achievable, where V_i ia an auxiliary random variable satisfying $V_i \to X_i \to Y, Z$, and V_{-i} denotes the collection $\{V_j, j \neq i\}$. Note that since $\mathbf{\Omega}$ is known at all the legitimate receivers and the eavesdropper, and since $\mathbf{V}_i$s are chosen to be independent of $\mathbf{\Omega}$, $\mathbf{\Omega}$ should appear in the conditioning of each of the mutual information quantities in (276). We keep this in mind, but drop it for the sake of notational simplicity.

First, we can upper bound the probability of error at each receiver. Let

$$V_i \triangleq \left(\mathbf{v}_{i1} \dots \mathbf{v}_{i(i-1)} \quad \mathbf{v}_{i(i+2)} \dots \mathbf{v}_{i(K+1)}\right) \tag{277}$$

Then, for any $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, then for almost all channel gains the average power constraint is satisfied and the probability of error is bounded by

$$\Pr(V_i \neq \hat{V}_i) \leq \exp\left(-\eta_{\gamma_i} P^{\delta}\right) \tag{278}$$

where η_{γ_i} is a positive constant which is independent of P and $\hat{V}_i$ is the estimate for V_i obtained by choosing the closest point in the constellation based on observation Y_i.

By Fano's inequality and the Markov chain $V_i \to Y_i \to \hat{V}_i$, we know that,

$$\begin{aligned}
I(V_i; Y_i) &\geq I(V_i; \hat{V}_i) && (279)\\
&= H(V_i) - H(V_i|\hat{V}_i) && (280)\\
&= \log(|\mathcal{V}_i|) - H(V_i|\hat{V}_i) && (281)\\
&\geq \log(|\mathcal{V}_i|) - 1 - \Pr(V_i \neq \hat{V}_i)\log(|\mathcal{V}_i|) && (282)\\
&= \left[1 - \Pr(V_i \neq \hat{V}_i)\right]\log(|\mathcal{V}_i|) - 1 && (283)\\
&= \log(|\mathcal{V}_i|) - o(\log P) && (284)\\
&= \frac{(K-1)M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (285)
\end{aligned}$$

where $o(\cdot)$ is the little-o function, $\mathcal{V}_i$ is the alphabet of V_i and, in this case, the cardinality of $\mathcal{V}_i$ is $(2Q+1)^{(K-1)M} = (2Q+1)^{(K-1)m^{K(K-1)+2}}$. Here, M is defined in (265).

Now, we bound the second term in (276). Let

$$U \triangleq \{\mathbf{u}_i, \tilde{\mathbf{u}}_i, i = 1, \dots, K\} \tag{286}$$

We have,

$$\begin{aligned}
I(V_i; Z|V_{-i}) &= I(V_i, U; Z|V_{-i}) - I(U; Z|V_1^K) && (287)\\
&= h(Z) - h(Z|U, V_1^K) - H(U|V_1^K) \\
&\quad + H(U|Z, V_1^K) && (288)\\
&\leq \frac{1}{2}\log P - h(N_Z) - H(U) + o(\log P) && (289)\\
&= \frac{1}{2}\log P - H(U) + o(\log P) && (290)\\
&= \frac{1}{2}\log P - \log(2Q+1)^{2KM} + o(\log P) && (291)\\
&= \frac{1}{2}\log P - \frac{(1-\delta)2KM}{2(M_S+\delta)}\log P + o(\log P) && (292)
\end{aligned}$$

Now, combining (285) and (292), we have,

$$R_i \geq \frac{(K-1)M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) - \frac{1}{2}\log P + \frac{(1-\delta)2KM}{2(M_S+\delta)}\log P + o(\log P) \quad (293)$$

By choosing δ small enough and choosing m large enough, we can make R_i arbitrarily close to $\frac{K-1}{2K}$. Thus, the sum s.d.o.f. of $\frac{K-1}{2}$ is achievable with fixed channel gains.

B. Fading Channel Gains

Here, we present a scheme that achieves $\frac{K-1}{2}$ s.d.o.f. using asymptotic vector space alignment with channel extension. Let $\Gamma = (K-1)^2$. We use $M_n = (K-1)n^\Gamma + (K+1)(n+1)^\Gamma$ channel uses to transmit $K(K-1)n^\Gamma$ message symbols securely to the legitimate receivers in the presence of the eavesdropper. Thus, we achieve a sum s.d.o.f. of $\frac{K(K-1)n^\Gamma}{(K-1)n^\Gamma+(K+1)(n+1)^\Gamma}$, which gets arbitrarily close to $\frac{K-1}{2}$ as $n \to \infty$.

First, we divide each message into many sub-messages; specifically, the message of the ith transmitter, W_i, is divided into $(K-1)$ sub-messages V_{ij}, $j = 1, \ldots, K+1$, $j \neq i, i+1$. Each V_{ij} is encoded into n^Γ independent streams $v_{ij}(1), \ldots, v_{ij}(n^\Gamma)$, which we denote as $\mathbf{v}_{ij} \stackrel{\Delta}{=} \left(v_{ij}(1), \ldots, v_{ij}(n^\Gamma)\right)^T$. We also require artificial noise symbols U_i and $\tilde{U}_i$ at each transmitter i. Again, we encode the artificial noise symbols U_i and $\tilde{U}_i$ as

$$\mathbf{u}_i \stackrel{\Delta}{=} \left(u_i(1), \ldots, u_i((n+1)^\Gamma)\right)^T, i = 1, \ldots, K \quad (294)$$

$$\tilde{\mathbf{u}}_i \stackrel{\Delta}{=} \left(\tilde{u}_i(1), \ldots, \tilde{u}_i(n^\Gamma)\right)^T, i = 1, \ldots, K-1 \quad (295)$$

$$\tilde{\mathbf{u}}_K \stackrel{\Delta}{=} \left(\tilde{u}_i(1), \ldots, \tilde{u}_i((n+1)^\Gamma)\right)^T \quad (296)$$

In each channel use $t \leq M_n$, we choose precoding column vectors $\mathbf{p}_{ij}(t)$, $\mathbf{q}_i(t)$ and $\tilde{\mathbf{q}}_i(t)$ with the same number of elements as $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. In channel use t, transmitter i sends

$$X_i(t) = \sum_j \mathbf{p}_{ij}(t)^T\mathbf{v}_{ij} + \mathbf{q}_i(t)^T\mathbf{u}_i + \tilde{\mathbf{q}}_i(t)^T\tilde{\mathbf{u}}_i \quad (297)$$

where we have dropped the limits on j in the summation for notational simplicity. By stacking the precoding vectors for all M_n channel uses, we let,

$$\mathbf{P}_{ij} = \begin{pmatrix} \mathbf{p}_{ij}(1)^T \\ \vdots \\ \mathbf{p}_{ij}^T(M_n) \end{pmatrix}, \quad \mathbf{Q}_i = \begin{pmatrix} \mathbf{q}_i(1)^T \\ \vdots \\ \mathbf{q}_i(M_n)^T \end{pmatrix} \quad (298)$$

and

$$\tilde{\mathbf{Q}}_i = \begin{pmatrix} \tilde{\mathbf{q}}_i(1)^T \\ \vdots \\ \tilde{\mathbf{q}}_i(M_n)^T \end{pmatrix} \quad (299)$$

Now, letting $\mathbf{X}_i = (X_i(1), \ldots, X_i(M_n))^T$, the channel input for all transmitter i over M_n channel uses can be compactly represented as

$$\mathbf{X}_i = \sum_j \mathbf{P}_{ij}\mathbf{v}_{ij} + \mathbf{Q}_i\mathbf{u}_i + \tilde{\mathbf{Q}}_i\tilde{\mathbf{u}}_i \quad (300)$$

Recall that, channel use t, the channel output at receiver l and the eavesdropper are, respectively, given by

$$Y_l(t) = \sum_{k=1}^K h_{kl}(t)X_k(t) + N_l(t) \quad (301)$$

$$Z(t) = \sum_{k=1}^K g_k(t)X_k(t) + N_Z(t) \quad (302)$$

Let $\mathbf{H}_{kl} \stackrel{\Delta}{=} \text{diag}\,(h_{kl}(1), \ldots, h_{kl}(M_n))$. Similarly, define $\mathbf{G}_k = \text{diag}\,(g_k(1), \ldots, g_k(M_n))$. The channel outputs at receiver l and the eavesdropper over all M_n channel uses, $\mathbf{Y}_l = (Y_l(1), \ldots, Y_l(M_n))^T$ and $\mathbf{Z} = (Z(1), \ldots, Z(M_n))^T$, respectively, can be represented by

$$\mathbf{Y}_l = \sum_{k=1}^K \mathbf{H}_{kl}\mathbf{X}_k + \mathbf{N}_l \quad (303)$$

$$= \sum_{k=1}^K \mathbf{H}_{kl}\left(\sum_{\substack{j=1\\ j\neq k,k+1}}^{K+1} \mathbf{P}_{kj}\mathbf{v}_{kj} + \mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_l \quad (304)$$

$$= \sum_{\substack{j=1\\ j\neq l,l+1}}^{K+1} \mathbf{H}_{ll}\mathbf{P}_{lj}\mathbf{v}_{lj} + \sum_{\substack{k=1\\ k\neq l}}^{K}\sum_{\substack{j=1\\ j\neq k,k+1}}^{K+1} \mathbf{H}_{kl}\mathbf{P}_{kj}\mathbf{v}_{kj} + \sum_{k=1}^K \mathbf{H}_{kl}\left(\mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_l \quad (305)$$

and,

$$\mathbf{Z} = \sum_{k=1}^K \mathbf{G}_k\mathbf{X}_k + \mathbf{N}_Z \quad (306)$$

$$= \sum_{k=1}^K \sum_{\substack{j=1\\ j\neq k,k+1}}^{K+1} \mathbf{G}_k\mathbf{P}_{kj}\mathbf{v}_{kj} + \sum_{k=1}^K \mathbf{G}_k\left(\mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_Z \quad (307)$$

Note that receiver l wants to decode $\mathbf{v}_{lj}$, $j = 1, \ldots, K+1$, $j \neq l, l+1$. Thus, the remaining terms in (305) constitute interference at the lth receiver. Recall that $CS(\mathbf{X})$ denotes the column space of the matrix $\mathbf{X}$. Then, I_l denoting the space spanned by this interference is

$$I_l = \left(\bigcup_{k\neq l, j\neq k,k+1} CS\left(\mathbf{H}_{kl}\mathbf{P}_{kj}\right)\right) \bigcup \left(\bigcup_{k=1}^K CS\left(\mathbf{H}_{kl}\mathbf{Q}_k\right)\right) \bigcup \left(\bigcup_{k=1}^K CS\left(\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k\right)\right) \quad (308)$$

Note that there are $(K-1)n^\Gamma$ symbols to be decoded by each legitimate receiver in $(K-1)n^\Gamma + (K+1)(n+1)^\Gamma$ channel uses. Thus, for decodability, the interference can occupy a subspace of rank at most $(K+1)(n+1)^\Gamma$, that is,

$$\text{rank}(I_l) \leq (K+1)(n+1)^\Gamma \quad (309)$$

To that end, we align the noise and message subspaces at each legitimate receiver appropriately. Note that no such alignment is possible at the external eavesdropper since the transmitters do not have its CSI. However, note that we have a total of $(K-1)n^{\Gamma}+(K+1)(n+1)^{\Gamma}$ artificial noise symbols which will span the full received signal space at the eavesdropper and secures all the messages.

Fig. 5 shows the alignment for $K = 3$ receivers. For the general K-user case, Fig. 7 shows the alignment in the interfering signal dimensions. At receiver l, it is as follows: First, the artificial noise symbols $\tilde{\mathbf{u}}_k$ is aligned with $\mathbf{u}_{k+1}$, for every $k = 1, \ldots, K-1$. Thus, we have,

$$\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k \preceq \mathbf{H}_{(k+1)l}\mathbf{Q}_{(k+1)}, \quad k = 1, \ldots, K-1 \tag{310}$$

where $\mathbf{A} \preceq \mathbf{B}$ is used to denote that $CS(\mathbf{A}) \subseteq CS(\mathbf{B})$. Thus, the subspace spanned by the artificial noise symbols can have a rank of at most $(K+1)(n+1)^{\Gamma}$.

The unwanted message symbols $\mathbf{v}_{kj}$, $k \neq l$, are aligned with $\mathbf{u}_j$ if $j \leq K$, or $\tilde{\mathbf{u}}_K$ otherwise. Thus,

$$\mathbf{H}_{kl}\mathbf{P}_{kj} \preceq \mathbf{H}_{jl}\mathbf{Q}_j, \quad j \leq K \tag{311}$$

$$\mathbf{H}_{kl}\mathbf{P}_{k(K+1)} \preceq \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K \tag{312}$$

for each $k \neq l$. Since, the unwanted messages at each receiver are aligned under the artificial noise subspaces, they do not increase the rank of I_l any further.

We can group the alignment equations for the artificial noise $\mathbf{u}_k$, $k = 1, \ldots, K$, and $\tilde{\mathbf{u}}_K$ for all K legitimate receivers. For $\mathbf{u}_1$, we have,

$$\mathbf{H}_{kl}\mathbf{P}_{k1} \preceq \mathbf{H}_{1l}\mathbf{Q}_1, \quad k \in \{2, \ldots, K\}, \ l \in \{1, \ldots, K\}, \ l \neq k \tag{313}$$

Clearly, these are $(K-1)^2$ alignment equations. Similarly, we have $(K-1)^2$ alignment equations for $\tilde{\mathbf{u}}_K$, given by

$$\mathbf{H}_{kl}\mathbf{P}_{k(K+1)} \preceq \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K, \quad k \in \{1, \ldots, K-1\}, \quad l \in \{1, \ldots, K\}, \ l \neq k \tag{314}$$

For the artificial noises $\mathbf{u}_k, k = 2, \ldots, K$, we have the following alignment equations:

$$\mathbf{H}_{(k-1)l}\tilde{\mathbf{Q}}_{k-1} \preceq \mathbf{H}_{kl}\mathbf{Q}_k \tag{315}$$

$$\mathbf{H}_{il}\mathbf{P}_{ik} \preceq \mathbf{H}_{kl}\mathbf{Q}_k, \quad i \neq k-1, k, \ l \neq i \tag{316}$$

Thus, there are $(K-1)^2 + 1$ alignment equations for each $\mathbf{u}_k, k = 2, \ldots, K$. Now we make the following selections:

$$\mathbf{P}_{k1} = \tilde{\mathbf{P}}_1, \quad k = 2, \ldots, K \tag{317}$$

$$\mathbf{P}_{k(K+1)} = \tilde{\mathbf{P}}_{K+1}, \quad k = 1, \ldots, K-1 \tag{318}$$

$$\mathbf{P}_{ik} = \tilde{\mathbf{P}}_k, \quad i \neq k-1, k, \quad k = 2, \ldots, K \tag{319}$$

$$\mathbf{H}_{(k-1)1}\tilde{\mathbf{Q}}_{k-1} = \mathbf{H}_{(k+1)1}\tilde{\mathbf{P}}_k, \quad k = 2, \ldots, K-1 \tag{320}$$

$$\mathbf{H}_{(K-1)2}\tilde{\mathbf{Q}}_{K-1} = \mathbf{H}_{12}\tilde{\mathbf{P}}_K \tag{321}$$

Now, note that it suffices to choose the matrices $\tilde{\mathbf{P}}_k$, $k = 1, \ldots, K+1$ in order to specify all the precoding matrices. Using these selections in our alignment equations in (313), (314), (315) and (316), we have $(K-1)^2$ alignment equations for each $\mathbf{u}_k$, $k = 1, \ldots, K$ and $\tilde{\mathbf{u}}_K$, given by,

$$\mathbf{T}_k\tilde{\mathbf{P}}_k \preceq \mathbf{Q}_k, \quad \mathbf{T}_k \in \tau_k, \quad k = 1, \ldots, K \tag{322}$$

$$\mathbf{T}_{K+1}\tilde{\mathbf{P}}_{K+1} \preceq \tilde{\mathbf{Q}}_K, \quad \mathbf{T}_{K+1} \in \tau_{K+1} \tag{323}$$

where the sets τ_k, $k = 1, \ldots, K+1$ are given by

$$\tau_1 = \Big\{\mathbf{H}_{1l}^{-1}\mathbf{H}_{kl}, k \in \{2, \ldots, K\}, l \in \{1, \ldots, K\}, l \neq k\Big\} \tag{324}$$

$$\tau_{K+1} = \Big\{\mathbf{H}_{Kl}^{-1}\mathbf{H}_{kl}, k \in \{1, \ldots, K-1\}, l \in \{1, \ldots, K\}, l \neq k\Big\} \tag{325}$$

$$\tau_k = \tau_k^P \bigcup \tau_k^Q \tag{326}$$

where,

$$\tau_k^P = \Big\{\mathbf{H}_{kl}^{-1}\mathbf{H}_{il}, i \notin \{k-1, k\}, l \neq i, l \in \{1, \ldots, K\}\Big\} \tag{327}$$

$$\tau_k^Q = \begin{cases} \Big\{\mathbf{H}_{kl}^{-1}\mathbf{H}_{(k-1)l}\mathbf{H}_{(k-1)1}^{-1}\mathbf{H}_{(k+1)1}, l \in \{1, \ldots, K\}\Big\}, \\ \qquad\qquad \text{if } k \in \{2, \ldots, K-1\} \\ \Big\{\mathbf{H}_{Kl}^{-1}\mathbf{H}_{(K-1)l}\mathbf{H}_{(K-1)2}^{-1}\mathbf{H}_{12}, l \in \{1, \ldots, K\}\Big\}, \\ \qquad\qquad \text{if } k = K \end{cases} \tag{328}$$

We can now construct the matrices $\tilde{\mathbf{P}}_k, k = 1, \ldots, K+1$, $\mathbf{Q}_k, k = 1, \ldots, K$ and $\tilde{\mathbf{Q}}_K$ as in [7]

$$\tilde{\mathbf{P}}_k = \left\{\left(\prod_{\mathbf{T} \in \tau_k} \mathbf{T}^{\alpha_T}\right)\mathbf{w}_k : \alpha_T \in \{1, \ldots, n\}\right\} \tag{329}$$

$$\mathbf{Q}_k = \left\{\left(\prod_{\mathbf{T} \in \tau_k} \mathbf{T}^{\alpha_T}\right)\mathbf{w}_k : \alpha_T \in \{1, \ldots, n+1\}\right\} \tag{330}$$

$$\tilde{\mathbf{Q}}_K = \left\{\left(\prod_{\mathbf{T} \in \tau_{K+1}} \mathbf{T}^{\alpha_T}\right)\mathbf{w}_{K+1} : \alpha_T \in \{1, \ldots, n+1\}\right\} \tag{331}$$

where each $\mathbf{w}_k$ is the $M_n \times 1$ column vector containing elements drawn independently from a continuous distribution with bounded support. This completes the description of our scheme.

Decodability: By our construction, the interference space at legitimate receiver l is given by,

$$I_l = \left(\bigcup_{k=1}^{K} CS(\mathbf{H}_{kl}\mathbf{Q}_k)\right) \bigcup \left(CS(\mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K)\right) \tag{332}$$

and clearly,

$$\text{rank}(I_l) \leq (K+1)(n+1)^{\Gamma} \tag{333}$$

We only need to show that desired signals $\mathbf{v}_{lj}$, $j \neq l, l+1$ fall outside I_l. The desired signal space at receiver l is given by

$$\mathbf{D}_l = \Big[\mathbf{H}_{ll}\tilde{\mathbf{P}}_1 \ldots \mathbf{H}_{ll}\tilde{\mathbf{P}}_{l-1} \quad \mathbf{H}_{ll}\tilde{\mathbf{P}}_{l+2} \ldots, \mathbf{H}_{ll}\tilde{\mathbf{P}}_K\Big] \tag{334}$$

We want to show that the matrix

$$\Lambda_l = \Big[\mathbf{D}_l \quad \tilde{\mathbf{I}}_l\Big] \tag{335}$$

where,

$$\tilde{\mathbf{I}}_l = \Big[\mathbf{H}_{1l}\mathbf{Q}_1 \ldots \mathbf{H}_{Kl}\mathbf{Q}_K \quad \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K\Big] \tag{336}$$

is full rank almost surely. To do so, we will use [34, Lemmas 1 and 2]. Note that the mth row of $\mathbf{H}_{kl}\mathbf{Q}_k$ contains the term w_{mk} with exponent 1, but no $w_{mk'}$ for $k \neq k'$, where w_{mk} denotes the element in the mth row of $\mathbf{w}_k$. In fact, the term w_{mk} occurs nowhere else in the matrix Λ_l except in $\mathbf{H}_{kl}\mathbf{Q}_k$ and $\mathbf{H}_{ll}\tilde{\mathbf{P}}_k$. This shows, using [34, Lemmas 1, 2], that $\mathbf{D}_l$ and $\tilde{\mathbf{I}}_l$ are full rank almost surely. Further, it suffices to show that the matrices $\begin{bmatrix}\mathbf{H}_{ll}\tilde{\mathbf{P}}_k & \mathbf{H}_{kl}\mathbf{Q}_k\end{bmatrix}, k = 1, \ldots, K$, and $\begin{bmatrix}\mathbf{H}_{ll}\tilde{\mathbf{P}}_{K+1} & \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K\end{bmatrix}$ are all full column rank. First, $\begin{bmatrix}\mathbf{H}_{ll}\tilde{\mathbf{P}}_1 & \mathbf{H}_{kl}\mathbf{Q}_1\end{bmatrix}$ is full column rank since $\mathbf{H}_{kl}\mathbf{Q}_1$ misses the term $\mathbf{H}_{ll}$. Similarly, $\begin{bmatrix}\mathbf{H}_{ll}\tilde{\mathbf{P}}_{K+1} & \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_1\end{bmatrix}$ is full column rank. Further, if $k \neq l, l+1$, $\mathbf{H}_{kl}\mathbf{Q}_k$ does not contain $\mathbf{H}_{ll}$ and hence $\begin{bmatrix}\mathbf{H}_{ll}\tilde{\mathbf{P}}_k & \mathbf{H}_{kl}\mathbf{Q}_k\end{bmatrix}$ is full column rank. Finally, note that the lth transmitter does not transmit any message signals along $\tilde{\mathbf{P}}_k$, when $k = l, l+1$. Thus, the matrix Λ_l is full rank almost surely. This ensures decodability of the desired signals at each receiver.

Security Guarantee: Let $\mathbf{v} = \{\mathbf{v}_{ij}, i, j \in \{1, \ldots, K\}, j \neq i, i+1\}$, that is, $\mathbf{v}$ is the collection of all legitimate messages to be secured from the eavesdropper. Also, let $\mathbf{u} = \{\mathbf{u}_k, \tilde{\mathbf{u}}_k, k = 1, \ldots, K\}$, that is $\mathbf{u}$ is the collection of all the artificial noise symbols. We note that

$$\begin{aligned} I(\mathbf{v}; \mathbf{Z}) &= h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{v}) && (337)\\ &\leq \frac{M_n}{2}\log P - h(\mathbf{A}\mathbf{u}) + o(\log P) && (338)\\ &= \frac{M_n}{2}\log P - \frac{M_n}{2}\log P + o(\log P) && (339)\\ &= o(\log P) && (340)\end{aligned}$$

where $\mathbf{A}$ is a $M_n \times M_n$ full rank matrix, and we have used Lemma 4 in (337). Also, we have implicitly used the fact that Ω appears in the conditioning of each mutual information and differential entropy term in the above calculation. Now, as before, by treating the vector channel with M_n slots as one channel use, and using wiretap channel codes, we get,

$$R_i \geq \frac{(K-1)n^{\Gamma}}{M_n}\log P + o(\log P) \qquad (341)$$

for each $i = 1, \ldots, K$, which gives us the required sum s.d.o.f. of $\frac{K(K-1)n^{\Gamma}}{(K-1)n^{\Gamma} + (K+1)(n+1)^{\Gamma}}$, which approaches $\frac{K-1}{2}$ as $n \to \infty$.

Appendix G
Achievable Scheme for the Multiple Access Wiretap Channel With Partial CSIT and Fading Channel Gains

We construct a scheme that achieves the desired sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ with fading channel gains. Without loss of generality, assume that the first m transmitters have eavesdropper CSI, while the remaining transmitters have no eavesdropper CSI. We provide a scheme to achieve the rate tuple $(d_1, \ldots, d_m, d_{m+1}, \ldots, d_K) = \left(\frac{K-1}{m(K-1)+1}, \ldots, \frac{K-1}{m(K-1)+1}, 0, \ldots, 0\right)$, thus, achieving the required sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$. For each $i = 1, \ldots, m$, transmitter i sends $\mathbf{V}_i = \left\{V_{ij},, j \neq i, j = 1, \ldots, K\right\}$ symbols in $m(K-1)+1$ time slots. Let $\mathbf{V} = \{\mathbf{V}_i, i = 1, \ldots, K\}$. Fig. 6 illustrates the alignment of the signals at the end of the scheme when $K = 3$ and $m = 2$. The scheme is as follows:

At time $t \in \{1, \ldots, m(K-1)+1\}$, the ith transmitter, $i = 1, \ldots, K$, sends,

$$X_i(t) = \begin{cases} \sum_{j=1, j\neq i}^{K} \frac{g_j(t)}{h_j(t)g_i(t)} V_{ij} + \frac{1}{h_i(t)} U_i, & 1 \leq i \leq m \\ \frac{1}{h_i(t)} U_i, & m+1 \leq i \leq K \end{cases} \qquad (342)$$

where U_i is an artificial noise symbol. This ensures that the noise symbols U_i all align at the legitimate receiver. On the other hand, the artificial noise symbol from the jth transmitter U_j protects all the messages V_{ij} for every i, at the eavesdropper. The channel outputs are given by,

$$Y(t) = \sum_{i=1}^{m}\sum_{j\neq i}\frac{h_i(t)g_j(t)}{h_j(t)g_i(t)}V_{ij} + \sum_{i=1}^{K}U_i + N_1(t) \qquad (343)$$

$$Z(t) = \sum_{i=1}^{K}\frac{g_i(t)}{h_i(t)}\left(U_i + \sum_{j=1, j\neq i}^{m}V_{ji}\right) + N_2(t) \qquad (344)$$

After the $m(K-1)+1$ time slots, the legitimate receiver ends up with $m(K-1)+1$ linearly independent equations with $m(K-1)+1$ variables: $\sum_{i=1}^{K} U_i$ and the $m(K-1)$ variables $\{V_{ij}\}$. Thus, it can decode all the $m(K-1)$ message symbols V_{ij}. Defining $\mathbf{Y} = \{Y(t),\ t = 1, \ldots, m(K-1)+1\}$ and $\mathbf{Z}$ similarly as $\mathbf{Y}$, this means that $I(\mathbf{V}; \mathbf{Y}) = m(K-1)\frac{1}{2}\log P + o(\log P)$, and also $I(\mathbf{V}; \mathbf{Z}) \leq o(\log P)$, concluding the achievability proof.

References

[1] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. 50th Annu. Allerton Conf. Commun. Contorl Comput. (Allerton)*, Oct. 2012, pp. 193–200.

[2] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[3] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 1337–1341.

[4] J. Xie and S. Ulukus, "Unified secure DoF analysis of K-user Gaussian interference channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 1107–1111.

[5] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[6] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. (Aug. 2009). "Real interference alignment with real numbers." [Online]. Available: https://arxiv.org/abs/0908.1208

[7] 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.

[8] A. S. Motahari, S. Oveis-Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4799–4810, Aug. 2014.

[9] A. G. Davoodi and S. A. Jafar. (Mar. 2014). "Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT." [Online]. Available: https://arxiv.org/abs/1403.1541

[10] S. Lashgari and A. S. Avestimehr, "Blind wiretap channel with delayed csit," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2014, pp. 36–40.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[12] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[13] S. 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.
[14] 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.
[15] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. New York, NY, USA: Springer, 2010, pp. 1–18.
[16] P. K. 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.
[17] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sep. 2010.
[18] P. Mukherjee and S. Ulukus, "Fading wiretap channel with no CSI anywhere," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 1347–1351.
[19] 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.
[20] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.
[21] R. Liu, I. Maric, P. Spasojević, and R. D. 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.
[22] 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.
[23] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[24] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.
[25] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.
[26] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
[27] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.
[28] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.
[29] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 246–255, Jan. 2014.
[30] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, Nov. 1997.
[31] G. Bresler and D. Tse, "The two user Gaussian interference channel: A deterministic view," *Eur. Trans. Telecommun.*, vol. 19, no. 4, pp. 333–354, Apr. 2008.
[32] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.
[33] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NJ, USA: Wiley, Jul. 2006.
[34] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom of wireless *X* networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3893–3908, Sep. 2009.

Pritam Mukherjee received his B. Tech (Hons.) with a major in Electronics and Electrical Communication Engineering and a minor in Computer Science and Engineering from Indian Institute of Technology (IIT), Kharagpur in 2010. Currently, he is pursuing a Ph.D in Electrical and Computer Engineering at the University of Maryland, College Park.

He received the Kulkarni Summer Research Fellowship at University of Maryland, College Park, in 2016. His research interests include information theoretic physical layer security and network information theory for wireless networks.

Jianwei Xie received his Ph.D. degree from the Department of Electrical and Computer Engineering at the University of Maryland, College Park in May 2014. Prior to that, he received the B.S. and M.S. degrees in electronic engineering from the Tsinghua University, Beijing, China, in 2006 and 2008, respectively. Currently, he is with Google Inc., Mountain View, CA USA.

He received the Distinguished Dissertation Fellowship from the ECE Department at the University of Maryland, College Park, in 2013. His research interests include information theory and wireless communications.

Sennur Ulukus (S'90–M'98–SM'15–F'16) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, and the Ph.D. degree in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University. Her research interests are in wireless communications, information theory, signal processing, networking, information theoretic physical layer security, and energy harvesting communications.

Dr. Ulukus is a Distinguished Scholar-Teacher of the University of Maryland. She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, the 2010-2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 ECE George Corcoran Education Award. She is on the Editorial Board of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS—Series on Green Communications and Networking (2015–2016) and the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING (2016). She was an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010) and the IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). SHE WAS A GUEST EDITOR FOR THE IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2015 and 2008), the *Journal of Communications and Networks* (2012), and the IEEE TRANSACTIONS ON INFORMATION THEORY (2011). She is a general TPC Co-Chair of the 2017 IEEE ISIT, the 2016 IEEE Globecom, the 2014 IEEE PIMRC, and the 2011 IEEE CTW.