Secure Degrees of Freedom Regions of Multiple Access and Interference Channels: The Polytope Structure

Jianwei Xie and Sennur Ulukus, *Senior Member, IEEE*

***Abstract*— In this paper, we determine the entire secure degrees of freedom (s.d.o.f.) regions of the K-user Gaussian multiple access (MAC) wiretap channel and the K-user interference channel (IC) with secrecy constraints. For the IC, we consider three secrecy constraints: K-user IC with an external eavesdropper (IC-EE), K-user IC with confidential messages (IC-CM), and their combination Kuser IC with confidential messages and external eavesdropper (IC-CM-EE). The converse for the IC includes constraints both due to secrecy as well as due to interference. For the IC, although the portion of the region close to the optimum sum s.d.o.f. point is governed by the upper bounds due to secrecy constraints, the other portions of the region are governed by the upper bounds due to interference constraints. Different from the existing literature, in order to fully understand the characterization of the s.d.o.f. region of the IC, one has to study the four-user case, i.e., the two- or three-user cases do not illustrate the full generality of the problem. In order to prove the achievability, we use the polytope structure of the converse region. In both MAC and IC cases, we develop explicit schemes that achieve the extreme points of the polytope region given by the converse. In particular, the extreme points of the MAC region are achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. The extreme points of the IC region are achieved by a $(K-m)$-user IC with confidential messages, m helpers, and N external eavesdroppers, for $m \geq 1$ and a finite N. A byproduct of our results in this paper is that the sum s.d.o.f. is achieved only at one extreme point of the s.d.o.f. region, which is the symmetric-rate extreme point, for both MAC and IC channel models.**

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

I. Introduction

IN THIS paper, we consider two fundamental multi-user network structures under secrecy constraints: K-user multiple access channel (MAC) and K-user interference channel (IC). Information-theoretic security of communication was first considered by Shannon in [1] via a noiseless wiretap channel. Noisy wiretap channel was introduced by Wyner who showed that information-theoretically secure communication was possible if the eavesdropper was degraded with respect to the legitimate receiver [2]. Csiszar and Korner generalized Wyner's result to arbitrary, not necessarily degraded, wiretap channels, and showed that information-theoretically secure communication was possible even when the eavesdropper was not degraded [3]. Leung-Yan-Cheong and Hellman extended Wyner's setting to a Gaussian channel, which is degraded [4]. This line of research has been extended to many multi-user scenarios, for both general and Gaussian channel models, see e.g., [5]–[26]. The secrecy capacity regions of most of these multi-user channels remain open problems even in simple Gaussian settings. In the absence of exact secrecy capacity regions, the behaviour of the secrecy rates at high signal-to-noise ratio (SNR) regimes have been studied by focusing on the secure degrees of freedom (s.d.o.f.), which is the pre-log of the secrecy rates, in [27]–[41].

In this paper, we focus on the K-user Gaussian MAC wiretap channel and the K-user Gaussian IC with secrecy constraints. The secrecy capacity regions of both of these models remain open. Early references [28]–[32] studied the sum s.d.o.f. of the MAC and IC models by developing achievable schemes. In particular, [28]–[30] achieved a sum s.d.o.f. of $\frac{K-1}{K}$ for the MAC wiretap channel; [31], [32] achieved a sum s.d.o.f. of $\frac{K(K-1)}{2K}$ for the IC-EE; and [31] achieved a sum s.d.o.f. of $\frac{K(K-2)}{2K-1}$ for the IC-CM. The best-known upper bounds for the MAC wiretap channel was 1, and for the IC-EE and IC-CM was $\frac{K}{2}$, which are the upper bounds for the corresponding non-secrecy settings [42]–[44]. References [28]–[32] directly applied interference alignment techniques to the secrecy settings. While interference alignment naturally provides some amount of secrecy due to aligning all unwanted signals in a separate dimension, in order to attain the optimum s.d.o.f., signals need to be designed more intricately. The *exact* sum s.d.o.f. of both of these channel models have been determined recently as $\frac{K(K-1)}{K(K-1)+1}$ for the MAC wiretap channel [45], [46], and as $\frac{K(K-1)}{2K-1}$ for the IC-EE and IC-CM [47], [48]. In particular, [45]–[48] utilize interference alignment together with intricately designed cooperative jamming signals to obtain the optimum sum s.d.o.f.

Manuscript received April 27, 2014; revised May 27, 2015; accepted September 30, 2015. Date of publication October 12, 2015; date of current version March 16, 2016. This work was supported by the National Science Foundation under Grant CNS 09-64632, Grant CCF 09-64645, Grant CCF 10-18185, and Grant CNS 11-47811. This paper was presented at the 2013 Asilomar Conference on Signals, Systems and Computers and the 2014 IEEE Information Theory Workshop.

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@google.com).

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

Communicated by Y. Liang, 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.2015.2490063

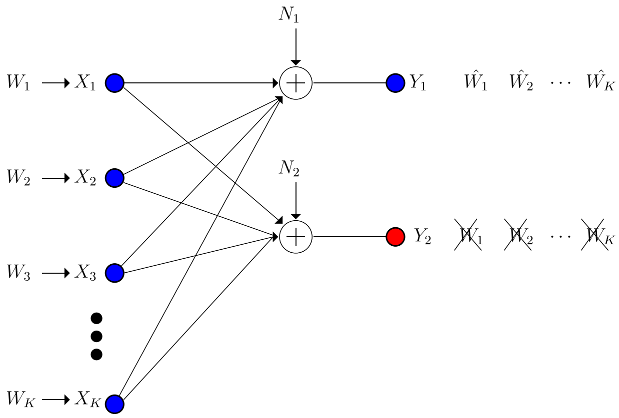

Fig. 1. K-user multiple access (MAC) wiretap channel.

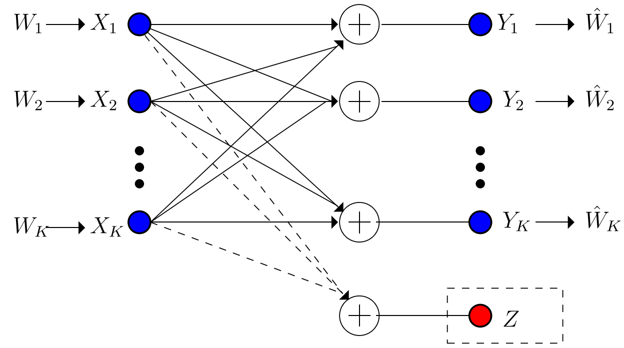

Fig. 2. K-user interference channel (IC) with secrecy constraints.

In this paper, we determine the *entire s.d.o.f. regions* of the MAC and IC models.

We start with the MAC wiretap channel, where multiple legitimate transmitters wish to have secure communication with a legitimate receiver in the presence of an eavesdropper; see Fig. 1. The converse for the *sum* s.d.o.f. is developed in [45] and [46] using two lemmas[1]: the *secrecy penalty lemma* [46, Lemma 1] and the *role of a helper lemma* [46, Lemma 2], which, respectively, quantify the rate penalty due to the existence of an eavesdropper, and quantify the impact of a helper (interferer) on the rate of another legitimate transmitter. The achievability for the sum s.d.o.f. in [45] and [46] is based on real interference alignment [49], [50] and structured cooperative jamming [14] with an emphasis on simultaneous alignments at both the legitimate receiver and the eavesdropper. We develop the converse for the *entire region* by starting from the converse proof given in [45] and [46] for the *sum* s.d.o.f. While [45] and [46] developed asymmetric upper bounds for the secure rates, since the sum s.d.o.f. was achieved by symmetric rates, [45], [46] summed up the asymmetric upper bounds to get a single symmetric upper bound to match the achievability. We revisit the converse proof in [45] and [46] and develop a converse for the entire region by keeping the developed asymmetric upper bounds. Therefore, the converse proofs developed in [45] and [46] to obtain a converse for the sum s.d.o.f. suffice to obtain a tight converse for the entire region.

The converse region for the s.d.o.f. problem has a general *polytope* structure, as opposed to the non-secrecy counterpart for the MAC which has a *polymatroid* structure [51]. Polytope is a bounded polyhedron, which is an intersection of a finite number of half-spaces. Such definition is called a half-space representation, which is exactly the way our converse is expressed. In order to show the achievability of the polytope region, we need to show the achievability of the boundaries of all of the half-spaces, which is inefficient. We use Minkowski theorem [52, Th. 2.4.5] which states that the polytope region discussed in this paper can be represented by the convex hull of all of its extreme points, which there are only finitely many. We, therefore, first determine the extreme points of this converse (polytope) region, and then develop an achievable scheme for each extreme point of the converse region; the achievability of the entire region then follows from time-sharing. In particular, each extreme point of the converse region is achieved by an m-user MAC wiretap channel with $K-m$ helpers, for $m = 1, \ldots, K$, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers.

We then consider the IC with secrecy constraints; see Fig. 2. In particular, we consider three different secrecy constraints in a unified framework as in [47] and [48]: 1) K-user IC with one external eavesdropper (IC-EE), where K transmitter-receiver pairs wish to have secure communication against an external eavesdropper. 2) K-user IC with confidential messages (IC-CM), where there are no external eavesdroppers, but each transmitter-receiver pair wishes to secure its communication against the remaining $K-1$ receivers. 3) K-user IC with confidential messages and one external eavesdropper (IC-CM-EE), which is a combination of the previous two cases, where each transmitter-receiver pair wishes to secure its communication against the $K-1$ receivers and the external eavesdropper. The converse for the *sum* s.d.o.f. (the sum s.d.o.f. is the same for all three models) was developed in [47] and [48] by using the *secrecy penalty* lemma and the *role of a helper* lemma in a certain way, and then by summing up the obtained asymmetric upper bounds into a single symmetric upper bound. The achievability for the sum s.d.o.f. in [47] and [48] is based on asymptotical real interference alignment [49] to enable simultaneous alignment at multiple receivers.

In order to develop a converse for the *entire region* for the IC case, similar to the MAC case, we start by re-examining the converse proof in [47] and [48] for the sum s.d.o.f. However, unlike the MAC case, the original steps used in [47] and [48] for the sum s.d.o.f. are not tight for the characterization of the entire region. There are two reasons for this: First, in the case of the MAC wiretap channel, since there is a single legitimate receiver, each transmitter (helper/interferer) impacts the total rate of all other legitimate transmitters at the legitimate receiver, and therefore, there is a single manner in which the *role of a helper* lemma is applied. In the IC case, there are many different ways in which the *role of a helper* lemma can be invoked as there are multiple receivers.

[1] These lemmas are stated and a brief discussion is provided in Section III-B for completeness.

In this case, by pairing up helpers (interferers) and the receivers we obtain $(K-1)^K$ upper bounds; even after removing the redundancies, we get $\left(\!\binom{K}{K-1}\!\right) = \binom{2K-2}{K-1}$ upper bounds.[2] In order to obtain the tightest subset of these upper bounds, we choose the most binding pairing of the helpers/interferers and the receivers. In particular, when developing the converse for the *sum* s.d.o.f. in [47], for each transmitter i, we applied the *role of a helper* lemma by choosing only one of its neighbors k ($k = i-1$ or $k = i+1$) as the helper/interferer. Instead, in this paper, we choose all of the transmitters as interfering with a single transmitter-receiver pair; see (124) and (141) in this paper. This yields the tightest upper bounds. Second, we observe that, when we study the s.d.o.f. region, we need to consider the non-secrecy upper bounds for the underlying IC [43], [44] as additional upper bounds. We note that such upper bounds are not needed for the s.d.o.f. region of the MAC wiretap channel, or the sum s.d.o.f. of MAC or IC. In fact, such non-secrecy upper bounds are not needed even for the s.d.o.f. region of the IC for the cases of $K = 2$ or $K = 3$. We observe that these upper bounds are needed for the IC with secrecy constraints starting with $K \geq 4$. To the best of our knowledge, this is the first time in network information theory that $K = 2$ or $K = 3$ do not capture the full generality of the problem, and we need to study $K = 4$ to observe a certain multi-user phenomenon to take effect.[3] That is, if one studied only $K = 2$ or $K = 3$ user cases, one might not have realized that interference constraints as well as secrecy constraints are needed in the s.d.o.f. region expressions for the IC; only after $K \geq 4$ do these constraints become binding. The intuitive reason for this is that for $K < 4$, interference constraints are implied by the secrecy constraints, whereas after $K \geq 4$, interference constraints introduce new constraints that are not represented by the secrecy constraints. For larger numbers of users, at the edges of the s.d.o.f. region, some users do not transmit messages but serve only as helpers by sending cooperative jamming signals; in such cases, decodabilitys at the legitimate receiver (interference) becomes a more dominant factor than secrecy at the eavesdropper.

The converse region for the IC with secrecy constraints has a *polytope* structure as well, and similar to the MAC wiretap channel case, we need to determine the extreme points of this polytope region. However, different from the MAC wiretap channel case, the converse region consists of two classes of upper bounds, due to secrecy and due to interference. This makes it difficult to identify the extreme points of the converse polytope. Finding the extreme points is related to finding full-rank sub-matrices from an overall matrix of size $2K + K(K-1)/2$. Since there are approximately K^K such matrices, an exhaustive search is intractable, and therefore we investigate the consistency of the upper bounds, which reduces the possible number of sub-matrices to examine. After determining the extreme points of the converse polytope, since most of the extreme points have multiple zero elements, in order to achieve them, it suffices to develop an achievable scheme for each extreme point by considering a $(K-m)$-user IC-CM with m helpers and N independent external eavesdroppers, for $m \geq 1$ and finite N. This is because, if there are m zero elements in an extreme point, then only $K-m$ transmitters need to have positive s.d.o.f., the remaining m transmitters will be helpers, and the corresponding m receivers become eavesdroppers, i.e., $N = 1 + m$.

Finally, after characterizing the entire s.d.o.f. regions of the MAC and IC with secrecy constraints, as a byproduct of our results in this paper, we note that the sum s.d.o.f. is achieved *only at one extreme point* of the s.d.o.f. region, which is the symmetric-rate extreme point, for both MAC and IC channel models.

[2]Here, $\left(\!\binom{n}{k}\!\right)$ is the multiset coefficient, which is equal to $\binom{n+k-1}{k}$.

[3]See an example of $K = 2$ not representing the full generality of the setting, and the need to study $K = 3$ to observe a phenomenon to take effect in [53].

II. System Model, Definitions and Results

A. K-User Gaussian MAC Wiretap Channel

The K-user Gaussian MAC wiretap channel (see Fig. 1) is:

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{1}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2 \tag{2}$$

where Y_1 is the channel output of the legitimate receiver, Y_2 is the channel output of the eavesdropper, X_i is the channel input of transmitter i, h_i and g_i are the channel gains of transmitter i to the legitimate receiver and the eavesdropper, respectively, and N_1 and N_2 are independent Gaussian random variables with zero-mean and unit-variance. All the channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_i and g_i are non-zero. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, K$.

Each transmitter i has a message W_i intended for the legitimate receiver. For each i, message W_i is uniformly and independently chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ where the n-length vector $\mathbf{X}_i \stackrel{\triangle}{=} X_i^n$ denotes the ith user's channel input in n channel uses. All messages are needed to be kept secret from the eavesdropper. A secrecy rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$ there exist n-length codes such that the legitimate receiver can decode the messages reliably, i.e., the probability of decoding error is less than ϵ

$$\Pr\left[(W_1, \ldots, W_K) \neq (\hat{W}_1, \ldots, \hat{W}_K)\right] \leq \epsilon \tag{3}$$

and the messages are kept information-theoretically secure against the eavesdropper

$$\frac{1}{n} H(W_1, \ldots, W_K|\mathbf{Y}_2) \geq \frac{1}{n} H(W_1, \ldots, W_K) - \epsilon \tag{4}$$

where $\hat{W}_1, \ldots, \hat{W}_K$ are the estimates of the messages based on observation $\mathbf{Y}_1$, where $\mathbf{Y}_1 \stackrel{\triangle}{=} Y_1^n$ and $\mathbf{Y}_2 \stackrel{\triangle}{=} Y_2^n$.

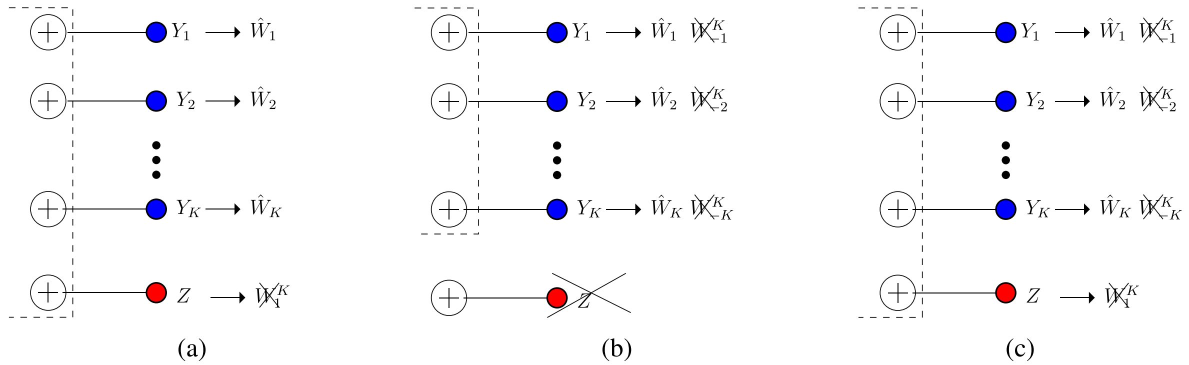

Fig. 3. The receiver sides of the three channel models: (a) K-user IC-EE, (b) K-user IC-CM, and (c) K-user IC-CM-EE, where $W_1^K \triangleq \{W_1, \ldots, W_K\}$ and $W_{-i}^K \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

The s.d.o.f. region is defined as:

$$D = \Big\{ \mathbf{d} : (R_1, \ldots, R_K) \text{ is achievable and } d_i \triangleq \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P},\ i = 1, \ldots, K \Big\} \quad (5)$$

where $\mathbf{d} = (d_1, \ldots, d_K)$.

The sum s.d.o.f. is defined as:

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \sup \frac{\sum_{i=1}^K R_i}{\frac{1}{2}\log P} \quad (6)$$

where the supremum is over all achievable secrecy rate tuples $(R_1, \ldots, R_K)$.

In this paper, we characterize the s.d.o.f. region of the K-user Gaussian MAC wiretap channel in the following theorem.

Theorem 1: The s.d.o.f. region D of the K-user Gaussian MAC wiretap channel is the set of all $\mathbf{d}$ *satisfying*

$$K d_i + (K-1) \sum_{j=1, j\neq i}^{K} d_j \leq K-1, \quad i = 1, \ldots, K \quad (7)$$

$$d_i \geq 0, \quad i = 1, \ldots, K \quad (8)$$

for almost all channel gains.

From the symmetry in Theorem 1, the sum s.d.o.f. is attained when $d_i = d, \forall i$. Using this in (7) gives the sum s.d.o.f. in the following corollary, which was originally proved in [46].

Corollary 1 ([46, Th. 1]): The sum s.d.o.f. of the K-user Gaussian MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$ for almost all channel gains.

B. K-User Gaussian IC With Secrecy Constraints

The K-user Gaussian IC with secrecy constraints (see Fig. 2) is:

$$Y_i = \sum_{j=1}^{K} h_{ji} X_j + N_i, \qquad i = 1, \ldots, K \quad (9)$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \quad (10)$$

where Y_i is the channel output of receiver i, Z is the channel output of the external eavesdropper (if there is any), X_i is the channel input of transmitter i, h_{ji} is the channel gain of the jth transmitter to the ith receiver, g_j is the channel gain of the jth transmitter to the eavesdropper (if there is any), and $\{N_1, \ldots, N_K, N_Z\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All the channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_{ji} are non-zero, and all g_j are non-zero if there is an external eavesdropper. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, K$.

Each transmitter i intends to send a message W_i, uniformly chosen from a set $\mathcal{W}_i$, to receiver i. The rate of message i is $R_i \triangleq \frac{1}{n}\log|\mathcal{W}_i|$, where n is the number of channel uses. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ to encode the message, where $\mathbf{X}_i \triangleq X_i^n$ is the n-length channel input of user i. The legitimate receiver j decodes the message as $\hat{W}_j$ based on its observation $\mathbf{Y}_j$. A secrecy rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$, there exist joint n-length codes such that each receiver j can decode the corresponding message reliably, i.e., the probability of decoding error is less than ϵ for all messages,

$$\max_j \Pr\left[W_j \neq \hat{W}_j\right] \leq \epsilon \quad (11)$$

and the corresponding secrecy requirement is satisfied. We consider three different secrecy requirements:

1) In IC-EE, Fig. 3(a), all of the messages are kept information-theoretically secure against the external eavesdropper,

$$\frac{1}{n} H(W_1, \ldots, W_K|\mathbf{Z}) \geq \frac{1}{n} H(W_1, \ldots, W_K) - \epsilon \quad (12)$$

2) In IC-CM, Fig. 3(b), all unintended messages are kept information-theoretically secure against each receiver,

$$\frac{1}{n} H(W_{-i}^K|\mathbf{Y}_i) \geq \frac{1}{n} H(W_{-i}^K) - \epsilon, \qquad i = 1, \ldots, K \quad (13)$$

where $W_{-i}^K \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

3) In IC-CM-EE, Fig. 3(c), all of the messages are kept information-theoretically secure against both

the $K-1$ unintended receivers and the eavesdropper, i.e., we impose both secrecy constraints in (12) and (13).

The s.d.o.f. region and the sum s.d.o.f. are defined as in (5) and (6).

In this paper, we characterize the s.d.o.f. region of the K-user IC-EE, IC-CM, and IC-CM-EE in the following theorem.

Theorem 2: The s.d.o.f. region D of K-user IC-EE, IC-CM, and IC-CM-EE is the set of all $\mathbf{d}$ *satisfying*

$$Kd_i + \sum_{j=1, j\neq i}^{K} d_j \leq K-1, \quad i = 1, \ldots, K \tag{14}$$

$$\sum_{i\in V} d_i \leq 1, \quad \forall\, V \subseteq \{1, \ldots, K\},\ |V| = 2 \tag{15}$$

$$d_i \geq 0, \quad i = 1, \ldots, K \tag{16}$$

for almost all channel gains.

From the symmetry in Theorem 2, the sum s.d.o.f. is attained when $d_i = d, \forall i$. Using this in (14) gives the sum s.d.o.f. in the following corollary, which was originally proved in [48].

Corollary 2 ([48, Th. 1]): The sum s.d.o.f. of the K-user Gaussian IC-EE, IC-CM, and IC-CM-EE is $\frac{K(K-1)}{2K-1}$ for almost all channel gains.

III. Preliminaries

A. Polytope Structure and Extreme Points

A set $P \subseteq R^n$ is a *polyhedron* if there is a system of finitely many inequalities $\mathbf{Hx} \leq \mathbf{h}$ such that

$$P = P(\mathbf{H}, \mathbf{h}) \stackrel{\triangle}{=} \left\{\mathbf{x} \in R^n \mid \mathbf{Hx} \leq \mathbf{h}\right\} \tag{17}$$

where $\mathbf{H}$ has n columns and an arbitrary number of rows, and $\mathbf{h}$ is a column vector.

The regions defined in Theorems 1 and 2 are bounded polyhedrons. We will study these polyhedrons by expressing all of their internal points in terms of their *extreme points*. First, we define a convex hull of points.

Let $X \subseteq R^n$. The *convex hull* of X, $\text{Co}(X)$, is the set of all convex combinations of the points in X:

$$\text{Co}(X) \stackrel{\triangle}{=} \left\{ \sum_i \lambda_i \mathbf{x}_i \mid \mathbf{x}_i \in X \text{ and } \sum_i \lambda_i = 1,\ \lambda_i \in R, \lambda_i \geq 0,\ \forall i \right\} \tag{18}$$

Next, we note that a set $P \subseteq R^n$ is a *polytope* if there is a finite set $X \subseteq R^n$ such that $P = \text{Co}(X)$. In addition, we have the following theorem.

Theorem 3 ([52, Th. 3.1.3]): Let $P \subseteq R^n$. Then, P is a bounded polyhedron if and only if P is a polytope.

Therefore, the regions defined in Theorems 1 and 2 are polytopes, and can be expressed as a convex hull of a finite set.

Further, if $P \subseteq R^n$ is a polytope, then it is a convex hull of some finite set X as stated above, and by the properties of the convex hull of a finite set X, P is a bounded, closed, convex set. Since P is a subset of the Euclidean space, P is a compact convex set. Minkowski theorem below states that such a set can be expressed as a convex hull of its extreme points.

Theorem 4 (Minkowski [52, Th. 2.4.5]): Let $P \subseteq R^n$ be a compact convex set. Then,

$$P = Co(Ex(P)). \tag{19}$$

An extreme point is formally defined as follows.

Definition 1 (Extreme Point): Let $P \subseteq R^n$. An $\mathbf{x} \in P$ is an extreme point if there are no $\mathbf{y}, \mathbf{z} \in P \setminus \{\mathbf{x}\}$ such that $\mathbf{x} = \lambda\mathbf{y} + (1-\lambda)\mathbf{z}$ for any $\lambda \in (0, 1)$. Then, $Ex(P)$ is the set of all extreme points of P.

Minkowski theorem plays an important role in this paper, since it tells that, instead of studying the polytope P itself, for certain problems, e.g., achievability proofs, we can simply concentrate on all extreme points $\text{Ex}(P)$.

Finally, the following theorem helps us find all extreme points of a polytope P efficiently: We select any n linearly independent active/tight boundaries and check whether they give a point in the polytope P.

Theorem 5 ([54, Th. 7.2(b)]): $\mathbf{x} \in R^n$ is an extreme point of polyhedron $P(\mathbf{H}, \mathbf{h})$ if and only if $\mathbf{Hx} \leq \mathbf{h}$ and $\mathbf{H}'\mathbf{x} = \mathbf{h}'$ for some $n \times (n+1)$ sub-matrix $(\mathbf{H}', \mathbf{h}')$ of $(\mathbf{H}, \mathbf{h})$ with rank$(\mathbf{H}') = n$, where $\mathbf{H}'$ is an $n \times n$ matrix and $\mathbf{h}'$ is a column vector.

B. Converse Tools: Secrecy Penalty and Role of a Helper

In this subsection, we review two lemmas that are used in the converse arguments. In the following lemma, we give a general upper bound for the secrecy rate. This lemma is first motivated by, and stated for, the Gaussian wiretap channel with M helpers [36], [46]. The goal of this lemma is to quantify the *secrecy penalty* due to the presence of an eavesdropper. Here, there is legitimate transmitter with channel input X_1, and M helpers with channel inputs X_2 through X_{M+1}, a legitimate receiver with channel output Y_1, and an eavesdropper with channel output Y_2. We work with n-letter signals (hence bold vectors) and introduce small independent Gaussian fudge variables $\tilde{N}_i$ and state inequalities in terms of slightly perturbed channel inputs $\tilde{X}_i$; this is for regularity purposes only, so that we can use differential entropies even for discrete signals.

This lemma states that the secrecy rate of the legitimate pair is upper bounded by the difference of the sum of differential entropies of all channel inputs (perturbed by small noise) and the differential entropy of the eavesdropper's observation; see (20). This upper bound can be interpreted as follows: If we consider the eavesdropper's observation as the *secrecy penalty,* then the secrecy penalty is tantamount to the elimination of one of the channel inputs in the system; see (21).

Lemma 1 (Secrecy Penalty Lemma [36], [46]): The secrecy rate of the legitimate pair is upper bounded as

$$nR \leq \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc \tag{20}$$

$$\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{21}$$

where $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ *for* $i = 1, 2, \cdots, M+1$, *and* $\tilde{\mathbf{N}}_i$ *is an i.i.d. sequence (in time) of random variables* $\tilde{N}_i$ *which are independent Gaussian random variables with zero-mean and variance* $\tilde{\sigma}_i^2$ *with* $\tilde{\sigma}_i^2 < \min(1/h_i^2, 1/g_i^2)$. *In addition,* c *and* c' *are constants which do not depend on* P, *and* $j \in \{1, 2, \cdots, M+1\}$ *could be arbitrary.*

In the following lemma, we give a general upper bound for the differential entropy of the signal of a helper based on the decodability of the message of the legitimate transmitter at the legitimate receiver. This lemma is also motivated in the helper setting, but as with Lemma 1 above, it is valid for more general settings [36], [46]. The goal of this lemma is to quantify the *role of a helper*, in terms of its affect on the system. In this lemma, W is the message of the legitimate transmitter, and its entropy $H(W)$ is the message rate. Here, X_j is the jth helper's channel input, and Y_1 is the legitimate receiver's channel output. Again, we use slightly perturbed channel inputs for regularity.

This lemma develops a constraint on the differential entropy of (the noisy version of) the cooperative jamming signal of any given helper, helper j in (22), in terms of the differential entropy of the legitimate user's channel output and the message rate $H(W)$. The inequality in (22) states that, for a given message rate $H(W)$, the entropy of the signal that the helper puts into the channel should not be too much. Alternatively, $H(W)$ can be moved to the left hand side of (22), and this inequality can be interpreted as an upper on the message rate given the helper signal's entropy. In particular, the higher the differential entropy of the cooperative jamming signal the lower this upper bound on the message rate will be.

Lemma 2 (Role of a Helper Lemma [36], [46]): For reliable de-coding at the legitimate receiver, the differential entropy of the input signal of helper j, $\mathbf{X}_j$, *must satisfy*

$$h(\mathbf{X}_j + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_1) - H(W) + nc \tag{22}$$

where c *is a constant which does not depend on* P, *and* $\tilde{N}$ *is a new Gaussian noise independent of all other random variables with* $\sigma_{\tilde{N}}^2 < \frac{1}{h_j^2}$, *and* $\tilde{\mathbf{N}}$ *is an i.i.d. sequence of* $\tilde{N}$.

C. Achievability Tools: Real Interference Alignment

In this subsection, we review pulse amplitude modulation (PAM) and real interference alignment [49], [50], similar to the review in [35, Sec. III]. The purpose of this subsection is to illustrate that by using real interference alignment, the transmission rate of a PAM scheme can be made to approach the Shannon achievable rate at high SNR. This provides a universal and convenient way to design capacity-achieving signalling schemes at high SNR by using PAM for different channel models as will be done in later sections.

1) Pulse Amplitude Modulation: For a point-to-point scalar Gaussian channel,

$$Y = X + Z \tag{23}$$

with additive Gaussian noise Z of zero-mean and variance σ^2, and an input power constraint $\mathrm{E}\left[X^2\right] \leq P$, assume that the input symbols are drawn from a PAM constellation,

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{24}$$

where Q is a positive integer and a is a real number to normalize the transmit power. Note that, a is also the minimum distance $d_{min}(C)$ of this constellation, which has the probability of error

$$\Pr(e) = \Pr\left[X \neq \hat{X}\right] \leq \exp\left(-\frac{d_{min}^2}{8\sigma^2}\right) = \exp\left(-\frac{a^2}{8\sigma^2}\right) \tag{25}$$

where $\hat{X}$ is an estimate for X obtained by choosing the closest point in the constellation $C(a, Q)$ based on observation Y.

The transmission rate of this PAM scheme is

$$R = \log(2Q + 1) \tag{26}$$

since there are $2Q + 1$ signalling points in the constellation. For any small enough $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2}}$ and $a = \gamma P^{\frac{\delta}{2}}$, where γ is a constant independent of P, then

$$\Pr(e) \leq \exp\left(-\frac{\gamma^2 P^\delta}{8\sigma^2}\right) \quad \text{and} \quad R \geq \frac{1-\delta}{2}\log P \tag{27}$$

and we can have $\Pr(e) \to 0$ and $R \to \frac{1}{2}\log P$ as $P \to \infty$. That is, we can have reliable communication at rates approaching $\frac{1}{2}\log P$.

Note that the PAM scheme has small probability of error (i.e., reliability) only when P goes to infinity. For arbitrary P, the probability of error $\Pr(e)$ is a finite number. Similar to the steps in [49] and [55], we connect the PAM transmission rate to the Shannon rate in the following derivation. We note that Shannon rate of $I(X; Y)$ is achieveable with arbitrary reliability using a random codebook:

$$\begin{aligned} R' &= I(X; Y) && (28)\\ &\geq I(X; \hat{X}) && (29)\\ &= H(X) - H(X|\hat{X}) && (30)\\ &= \log(2Q+1) - H(X|\hat{X}) && (31)\\ &\geq \log(2Q+1) - 1 - \Pr(e)\log(2Q+1) && (32)\\ &\geq \left[1 - \Pr(e)\right]\frac{1-\delta}{2}\log P - 1 && (33) \end{aligned}$$

where we use the Markov chain $X \to Y \to \hat{X}$ and bound $H(X|\hat{X})$ using Fano's inequality. Therefore, we can achieve the rate in (33) with arbitrary reliability, where for any fixed P, $\Pr(e)$ in (33) is the probability of error of the PAM scheme given in (27), which is a well-defined function of P. For a finite P, while $\Pr(e)$ may not be arbitrarily small, the rate achieved in (33), which is smaller than the rate of PAM in (26), is achieved arbitrarily reliably. We finally note that as P goes to infinity $\Pr(e)$ goes to zero exponentially, and from (33), both PAM transmission rate and the Shannon achievable rate have the same asymptotical performance.

2) Real Interference Alignment: This PAM scheme for the point-to-point scalar channel can be generalized to multiple data streams. Let the transmit signal be

$$x = \mathbf{a}^T\mathbf{b} = \sum_{i=1}^{L} a_i b_i \tag{34}$$

where $a_1, \ldots, a_L$ are rationally independent real numbers[4] and each b_i is drawn independently from the constellation $C(a, Q)$ in (24). The real value x is a combination of L data streams, and the constellation observed at the receiver consists of $(2Q+1)^L$ signal points.

By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, [49], [50] bounded the minimum distance d_{min} of points in the receiver's constellation: For any $\delta > 0$, there exists a constant k_δ, such that

$$d_{min} \geq \frac{k_\delta a}{Q^{L-1+\delta}} \tag{35}$$

for almost all rationally independent $\{a_i\}_{i=1}^L$, except for a set of Lebesgue measure zero. Since the minimum distance of the receiver constellation is lower bounded, with proper choice of a and Q, the probability of error can be made arbitrarily small, with rate R approaching $\frac{1}{2}\log P$. This result is stated in the following lemma, as in [35, Proposition 3].

Lemma 3 ([49], [50]): For any small enough $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose

$$Q = P^{\frac{1-\delta}{2(L+\delta)}} \quad \text{and} \quad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{36}$$

then the average power constraint is satisfied, i.e., $E\left[X^2\right] \leq P$, and for almost all $\{a_i\}_{i=1}^L$, except for a set of Lebesgue measure zero, the probability of error is bounded by

$$\Pr(e) \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{37}$$

where η_γ is a positive constant which is independent of P.

Furthermore, as a simple extension, if b_i are sampled independently from different constellations $C_i(a, Q_i)$, the lower bound in (35) can be modified as

$$d_{min} \geq \frac{k_\delta a}{(\max_i Q_i)^{L-1+\delta}} \tag{38}$$

IV. s.d.o.f. Region of K-User MAC Wiretap Channel

In this section, we study the K-user MAC wiretap channel defined in Section II-A and prove the s.d.o.f. region stated in Theorem 1. We first illustrate the regions for $K = 2$ and $K = 3$ cases as examples. We then provide the converse in Section IV-A, investigate the converse region in terms of its extreme points in Section IV-B, and show the achievability of each extreme point in Section IV-C.

For $K = 2$, the s.d.o.f. region in Theorem 1 becomes

$$\begin{aligned} D = \Big\{\mathbf{d} : 2d_1 + d_2 &\leq 1, \\ d_1 + 2d_2 &\leq 1, \\ d_1, d_2 &\geq 0\Big\} \end{aligned} \tag{39}$$

and is shown in Fig. 4. The extreme points of this region are: $(0,0)$, $(\frac{1}{2}, 0)$, $(0, \frac{1}{2})$, and $(\frac{1}{3}, \frac{1}{3})$. In order to provide the achievability of the region, it suffices to provide the achievability of these extreme points. In fact the achievabilities of $(\frac{1}{2}, 0)$, $(0, \frac{1}{2})$ were proved in [36] and [46] in the helper setting and the achievability of $(\frac{1}{3}, \frac{1}{3})$ was proved in [45] and [46]. Note that $(\frac{1}{3}, \frac{1}{3})$ is the only sum s.d.o.f. optimum point.

[4] $a_1, \ldots, a_L$ are rationally independent if whenever $q_1, \ldots, q_L$ are rational numbers then $\sum_{i=1}^L q_i a_i = 0$ implies $q_i = 0$ for all i.

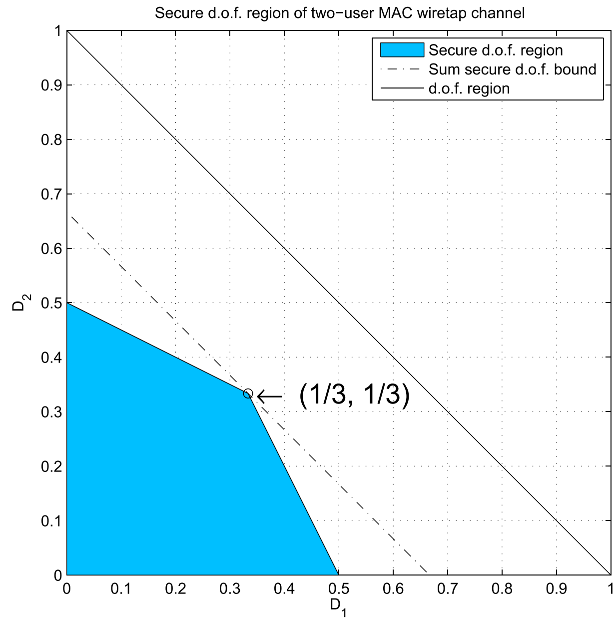

Fig. 4. The s.d.o.f. region of the $K = 2$-user MAC wiretap channel.

For $K = 3$, the s.d.o.f. region in Theorem 1 becomes

$$\begin{aligned} D = \Big\{\mathbf{d} : 3d_1 + 2d_2 + 2d_3 &\leq 2, \\ 2d_1 + 3d_2 + 2d_3 &\leq 2, \\ 2d_1 + 2d_2 + 3d_3 &\leq 2, \\ d_1, d_2, d_3 &\geq 0\Big\} \end{aligned} \tag{40}$$

and is shown in Fig. 5. The extreme points of this region are:

$$\begin{aligned} &\left(0,0,0\right) \\ &\left(\frac{2}{3},0,0\right), \left(0,\frac{2}{3},0\right), \left(0,0,\frac{2}{3}\right) \\ &\left(\frac{2}{5},\frac{2}{5},0\right), \left(\frac{2}{5},0,\frac{2}{5}\right), \left(0,\frac{2}{5},\frac{2}{5}\right) \\ &\left(\frac{2}{7},\frac{2}{7},\frac{2}{7}\right) \end{aligned} \tag{41}$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers [36], [46]), the maximum sum of pair of s.d.o.f. (see two-user Gaussian MAC wiretap channel with one helper, proved in Section IV-C), and the maximum sum s.d.o.f. (see three-user Gaussian MAC wiretap channel [45], [46]). Note that $(\frac{2}{7}, \frac{2}{7}, \frac{2}{7})$ is the only sum s.d.o.f. optimum point.

Regarding the region in Theorem 1, as illustrated in the examples above, we provide a few general comments here: First, we note that, without secrecy constraints, i.e., with only decodability constraints, the d.o.f. region is simply $\sum_{j=1}^K d_j \leq 1$. In contrast, the region in Theorem 1 is strictly dominated by the upper bounds due to secrecy constraints.

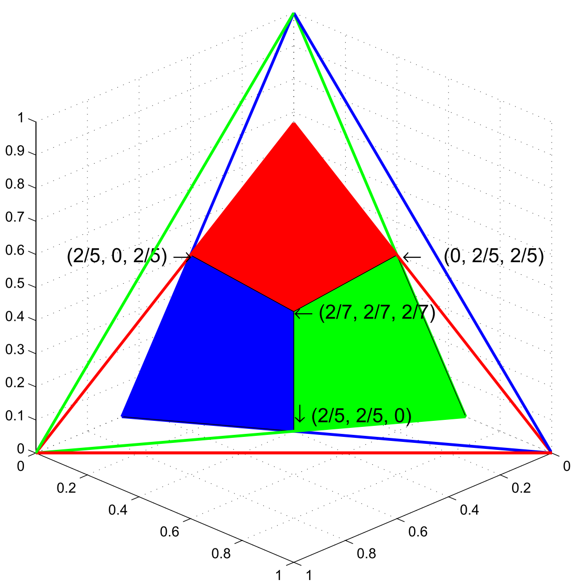

Fig. 5. The s.d.o.f. region of the $K = 3$-user MAC wiretap channel.

Second, we note that the pattern of the extreme points is that they all have $K - m$ zero components (these users do not send messages, they act as pure helpers), while the rest of the m users get equal individual s.d.o.f., which also correspond to the maximum sum s.d.o.f. for these m users. This will motivate the achievability proof in Section IV-C.

A. Converse

In order to prove the converse of the K-user MAC, we start with a multi-user version of the secrecy penalty lemma[5]:

$$n \sum_{i=1}^{K} R_i \leq \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_2) + nc_1 \tag{42}$$

$$\leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_2 \tag{43}$$

where all $\{c_i\}$ in this paper are constants independent of P. In addition, from the multi-user version of the role of a helper lemma,[6] we have, for each j,

$$h(\tilde{\mathbf{X}}_j) \leq h(\mathbf{Y}_1) - \sum_{i \neq j} H(W_i) + nc_3 \tag{44}$$

Then, combing (43) and (44), we have

$$n \sum_{i=1}^{K} R_i \leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_4 \tag{45}$$

$$\leq \sum_{j=2}^{K} \left[h(\mathbf{Y}_1) - \sum_{i \neq j} H(W_i) \right] + nc_5 \tag{46}$$

[5]Single-user version of the secrecy penalty lemma and the role of a helper lemma are reviewed in Section III-B. Equations (42)-(43) are the *multi-user* version in the sense that we have the sum of rates on the left hand side, compared to (20)-(21). A detailed proof of the multi-user version of the secrecy penalty lemma can be found in [46, Sec. IX].

[6]Multi-user version because we have sum of all rates but the jth on the right hand side of (44), compared to (22). A detailed proof of the multi-user version of the role of a helper lemma can be found in [46, Sec. IX].

Noting that $H(W_i) = nR_i$, this is equivalent to:

$$nR_i + (K-1) \sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_6 \tag{47}$$

where $i = 1, \ldots, K$.

Clearly, (47) is not symmetric. However, the lower bound derived in [46] was achieved by a symmetric scheme. Therefore, in [46], in order to obtain a matching upper bound for sum s.d.o.f., we summed up (47) for all i to obtain:

$$[K(K-1)+1] \sum_{j=1}^{K} nR_j \leq K(K-1)h(\mathbf{Y}_1) + nc_7 \tag{48}$$

$$\leq K(K-1)\frac{n}{2} \log P + nc_8 \tag{49}$$

which provided the desired upper bound for the sum s.d.o.f.

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \tag{50}$$

which is the converse for Corollary 1.

In fact, (47) provides more information than what is needed for the sum s.d.o.f. only. In this paper, we start from (47)

$$nR_i + (K-1) \sum_{j=1}^{K} nR_j \leq (K-1) \left(\frac{n}{2} \log P \right) + nc_9 \tag{51}$$

divide by $\frac{n}{2} \log P$ and take the limit $P \to \infty$ on both sides to obtain,

$$d_i + (K-1) \sum_{j=1}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{52}$$

that is,

$$Kd_i + (K-1) \sum_{j=1, j \neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{53}$$

which concludes the converse proof of Theorem 1.

B. Polytope Structure and Extreme Points

To prove that the region D in Theorem 1 is tight (i.e., achievable), we first express it in terms of its *extreme points*, explicitly characterize all of its extreme points, and develop a scheme to achieve each of its extreme points.

The region in Theorem 1 is a polytope, which is a convex hull of some finite set X, as discussed in Section III-A. By the properties of the convex hull of a finite set X, D is a bounded, closed, convex set. Since $D \subset R^K$, D is a compact convex set. From Minkowski theorem, the polytope D in Theorem 1 is a convex hull of its extreme points. Then, in order to prove that D is tight, it suffices to prove that each extreme point of D is achievable. Then, from convexification through time-sharing, all points in D are achievable.

In order to speak of the polytope, we re-write the constraints in (7) and (8) as

$$Kd_i + (K-1) \sum_{j=1, j \neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{54}$$

$$-d_i \leq 0, \qquad i = 1, \ldots, K \tag{55}$$

Then, we write all the left hand sides of (54) and (55) as an $N \times K$ matrix $\mathbf{H}$ with corresponding right hand sides forming an N-length column vector $\mathbf{h}$, i.e., all points $\mathbf{d}$ in D satisfy

$$\mathbf{Hd} \leq \mathbf{h} \tag{56}$$

where $N \triangleq 2K$. By Theorem 5, exploring all extreme points of D is equivalent to finding all sub-matrices $(\mathbf{H}_J, \mathbf{h}_J)$ of $(\mathbf{H}, \mathbf{h})$, such that

$$\text{rank}(\mathbf{H}_J) = K \tag{57}$$

and

$$\mathbf{H}_J\mathbf{d} = \mathbf{h}_J, \quad \text{and} \quad \mathbf{Hd} \leq \mathbf{h} \tag{58}$$

where $\mathbf{H}_J$ is a sub-matrix of $\mathbf{H}$ with rows indexed by the index set J, and $\mathbf{h}_J$ is the sub-vector of $\mathbf{h}$ with rows indexed by J.

Let $\mathbf{d} \in D$ be a non-zero extreme point of D. Define a subset $S \subseteq \{1, \ldots, N\}$ as

$$\begin{aligned} S \triangleq \Big\{ s_i \triangleq s(i) : \mathbf{H}_{s_i}\mathbf{d} = \mathbf{h}_{s_i} \text{ such that} \\ K d_i + (K-1) \sum_{j=1, j \neq i}^{K} d_j = K - 1, \\ i \in \{1, \ldots, K\} \Big\} \end{aligned} \tag{59}$$

where $s(i)$ is a function of the coordinate i with the value as the row index of $\mathbf{H}$ corresponding to the active boundaries in (54). Similarly, define the set $Z \subseteq \{1, \ldots, N\}$ as

$$\begin{aligned} Z \triangleq \Big\{ z_i \triangleq z(i) : \mathbf{H}_{z_i}\mathbf{d} = \mathbf{h}_{z_i} \text{ such that} \\ d_i = 0, \quad i \in \{1, \ldots, K\} \Big\} \end{aligned} \tag{60}$$

where $z(i)$ is a function of the coordinate i with the value as the row index of $\mathbf{H}$ corresponding to the active boundaries in (55). Clearly, S and Z are disjoint, i.e.,

$$S \cap Z = \phi \tag{61}$$

For any row index set J, which corresponds to a set of active boundaries for $\mathbf{d}$, we have

$$J = S \cup Z \tag{62}$$

For example, for the three-user case, $K = 3$, according to (54) and (55), we have $\mathbf{H}$ and $\mathbf{h}$ as

$$\mathbf{H} = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \mathbf{h} = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{63}$$

If the equalities with $i = 1, 2$ hold in (54) and the equality with $i = 3$ holds in (55), then the corresponding sets S, Z, J are

$$S = \{s_1, s_2\} = \{1, 2\} \tag{64}$$

$$Z = \{z_3\} = \{6\} \tag{65}$$

$$J = S \cup Z = \{1, 2, 6\} \tag{66}$$

with the row-index functions

$$s_i = s(i) = i \tag{67}$$

$$z_i = z(i) = i + 3 \tag{68}$$

In this example, it is easy to check that

$$\text{rank}(\mathbf{H}_J) = \text{rank}\left(\begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 0 & 0 & -1 \end{bmatrix} \right) = 3 = K \tag{69}$$

and the solution given by $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$ is

$$\mathbf{d} = \left(\frac{2}{5}, \frac{2}{5}, 0 \right) \tag{70}$$

which satisfies (58). Therefore, this is an extreme point.

For the general case, we have the following theorem.

Theorem 6: A point $\mathbf{d} \in D$ of Theorem 1 is an extreme point if and only if it is equal to, up to element reordering,

$$\Big(\underbrace{\Delta, \ldots, \Delta}_{m \text{ items}}, \underbrace{0, \ldots, 0}_{(K-m) \text{ items}} \Big), \quad 0 \leq m \leq K \tag{71}$$

where

$$\Delta = \frac{K-1}{m(K-1)+1} \tag{72}$$

Proof: First, for any m, $0 \leq m \leq K$, let the point $\mathbf{d}$ be as in (71). It is easy to check that the sub-matrix $(\mathbf{H}_J, \mathbf{h}_J)$, where

$$J = \Big\{ s_i : 1 \leq i \leq m \Big\} \cup \Big\{ z_j : m+1 \leq j \leq K \Big\} \tag{73}$$

satisfies all the conditions in Theorem 5, which means that $\mathbf{d}$ is an extreme point.

In order to show the other direction, we need to show that any extreme point $\mathbf{d}$ has the structure in (71) for some m, $0 \leq m \leq K$. To this end, we find the sub-matrix in Theorem 5.

If $|Z| = K$, due to (55), the sub-matrix $\mathbf{H}_Z$ is simply a diagnoal matrix with -1s on the diagonal, and consequently, $\text{rank}(\mathbf{H}_Z) = K$. Then, the solution of $\mathbf{H}_Z\mathbf{d} = \mathbf{h}_Z$ is $\mathbf{0}$, which satisfies (58). This extreme point corresponds to the case $m = 0$ in Theorem 6.

In the rest of the proof, we focus on non-zero extreme points, i.e., $|Z| < K$. Due to (54), it is easy to verify that $\mathbf{H}_S$ has $|S|$ rows with $\text{rank}(\mathbf{H}_S) = |S|$ where S is defined in (59). In order to make $\text{rank}(\mathbf{H}_J) = \text{rank}(\mathbf{H}_{S \cup Z}) = K$, we need at least $K - |S|$ more rows from $\mathbf{H}$, i.e., $|Z| \geq K - |S|$. If S is empty, then $|Z| \geq K$, which contradicts the assumption $|Z| < K$. Therefore, S is non-empty, i.e., $|S| \geq 1$.

First, we claim that

$$d_i = d_k, \quad \forall s_i, s_k \in S \tag{74}$$

If $|S| = 1$, there is nothing to prove, and the proof of (74) is completed. If $|S| > 1$, consider any $s_i, s_k \in S$, $i \neq k$. By the definition of S, we have

$$(K-1)d_k + K d_i + (K-1) \sum_{l \neq i,k} d_l = K - 1 \tag{75}$$

$$(K-1)d_i + K d_k + (K-1) \sum_{l \neq i,k} d_l = K - 1 \tag{76}$$

which implies that $d_i = d_k$ for any $s_i, s_k \in S$, proving (74) for $|S| \geq 1$.

Next, we claim

$$d_i > 0, \quad \forall s_i \in S \tag{77}$$

If $|S| = K$, due to (74), (77) is trivially true since we are focusing on a non-zero extreme point. If $|S| < K$, then we observe that

$$d_i \geq d_j, \qquad \forall s_i \in S, s_j \notin S \tag{78}$$

which indicates that for any $s_i \in S$ the corresponding element in vector $\mathbf{d}$ is the largest one, i.e., $d_i = \max_k d_k$, which implies (77). Hence, it now suffices to show (78). We prove it by contradiction. Assume that there exists a coordinate j such that $s_j \notin S$ and d_j is strictly larger than d_i for any $s_i \in S$. By the definition of S in (59), we have

$$K-1 = Kd_i + (K-1)d_j + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l \tag{79}$$

$$< Kd_i + (K-1)d_j + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l + (d_j - d_i) \tag{80}$$

$$= Kd_j + (K-1)d_i + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l \tag{81}$$

$$= Kd_j + (K-1)\sum_{l=1,l\neq j}^{K} d_l \tag{82}$$

which contradicts the constraint (54). Therefore, we must have (78) and consequently (77).

Finally, denote $m \stackrel{\triangle}{=} |S|$, and, without loss of generality, assume that $S = \{s_i : 1 \leq i \leq m\}$. By (77) and the definition of Z in (60), we note that $z_j \in Z$ only if $s_j \notin S$. Together with the constraint $|Z| \geq K - |S| = K - m$, we conclude that we must have $Z = \{z_j : m+1 \leq j \leq K\}$, i.e., $d_j = 0$ for $m+1 \leq j \leq K$. Thus, $\text{rank}(\mathbf{H}_{S\cup Z}) = K$, and, by (74), the solution given by the corresponding equations can be characterized as (71), which satisfies (58), completing the proof. ∎

C. Achievability

The previous section showed that the converse region is a polytope with extreme points which have m coordinates all equal to Δ given in (72), and the remaining $K-m$ coordinates all equal to zero. It is clear that zero vector is an extreme point in D and is trivially achievable. The rest of the achievability proof focuses on non-zero extreme points. In this section, we prove that each of these extreme points is achievable. Without loss of generality, we prove that the s.d.o.f. point of

$$\mathbf{d} = \Big(\underbrace{\Delta,\ldots,\Delta}_{m \text{ items}},\ \underbrace{0,\ldots,0}_{(K-m) \text{ items}}\Big) \tag{83}$$

is achievable for all $1 < m < K$ with Δ in (72). By symmetry, this proves the achievability of all extreme points. Note that $m = K$ is shown in [45] and [46], and $m = 1$ is shown in [36].

Theorem 7: The extreme point $\mathbf{d} \in D$ *given in (83) is achieved by* m*-user Gaussian MAC wiretap channel with* $K-m$ *helpers for almost all channel gains.*

Proof: Consider the m-user Gaussian MAC wiretap channel with $K-m$ helpers where transmitter i, $i = 1,\ldots,m$, has confidential message W_i intended for the legitimate receiver and the remaining $K-m$ transmitters serve as independent helpers without messages of their own.

In order to achieve the extreme point $\mathbf{d}$ in (83), transmitter i, $i = 1,\ldots,m$, divides its message into $K-1$ mutually independent sub-messages. Each transmitter sends a linear combination of signals that carry the sub-messages. In addition to message carrying signals, all transmitters also send cooperative jamming signals U_i, $i = 1,\ldots,K$, respectively. The messages are sent in such a way that all of the cooperative jamming signals are aligned in a single dimension at the legitimate receiver, occupying the smallest possible space at the legitimate receiver, and hence allowing for the reliable decodability of the message carrying signals. In addition, each cooperative jamming signal is aligned with at most $K-1$ message carrying signals at the eavesdropper to limit the information leakage rate to the eavesdropper. An example of $K = 3$, $m = 2$, and $K-m = 1$ is given in Fig. 6.

More specifically, we use a total of $m(K-1)+K$ mutually independent random variables

$$V_{ij}, \quad i \in \{1,\ldots,m\}, \quad j \in \{1,\cdots,K\}\setminus\{i\} \tag{84}$$

$$U_k, \quad k \in \{1,\cdots,K\} \tag{85}$$

where $\{V_{ij}\}_{j\neq i}$ denote the message carrying signals and U_i denotes the cooperative jamming signal sent from transmitter i. In particular, V_{ij} carries the jth sub-message of transmitter i. Each of these random variables is uniformly and independently drawn from the same discrete constellation $C(a, Q)$ given in (24), where a and Q will be specified later. We choose the input signals of the transmitters as

$$X_i = \sum_{j=1,j\neq i}^{K} \frac{g_j}{h_j g_i} V_{ij} + \frac{1}{h_i} U_i, \qquad i \in \{1,\ldots,m\} \tag{86}$$

$$X_j = \frac{1}{h_j} U_j, \qquad j \in \{m+1,\ldots,K\} \tag{87}$$

With these input selections, observations of the receivers are

$$Y_1 = \left[\sum_{i=1}^{m}\sum_{j=1,j\neq i}^{K} \frac{g_j h_i}{h_j g_i} V_{ij}\right] + \left(\sum_{k=1}^{K} U_k\right) + N_1 \tag{88}$$

and

$$Y_2 = \sum_{j=1}^{K} \frac{g_j}{h_j}\left(U_j + \sum_{i=1,i\neq j}^{m} V_{ij}\right) + N_2 \tag{89}$$

where the terms inside the parentheses $(\cdot)$ in (88) and (89) are *aligned*.

By [29, Th. 1], we can achieve the following sum secrecy rate for the m users

$$\sup \sum_{i=1}^{m} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{90}$$

where $\mathbf{V} \stackrel{\triangle}{=} \{V_{ij} : i \in \{1,\ldots,m\},\ j \in \{1,\cdots,K\}\setminus\{i\}\}$.

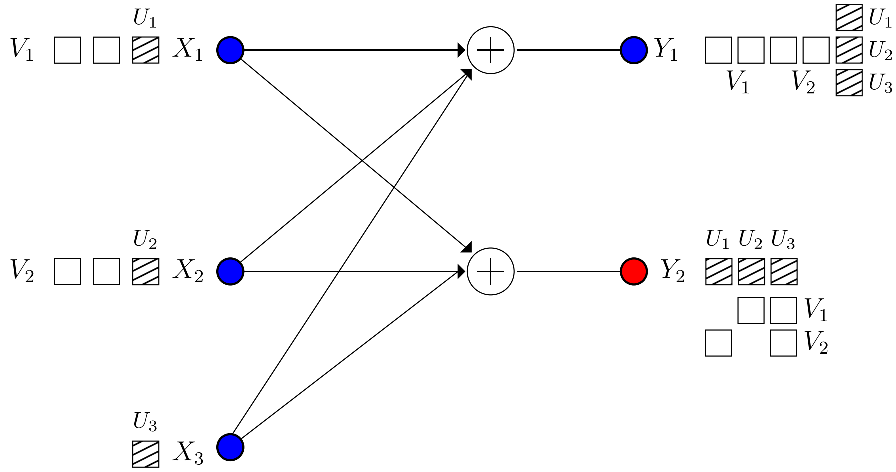

Fig. 6. Illustration of secure interference alignment for the s.d.o.f. triple $(\frac{2}{5}, \frac{2}{5}, 0)$ for the two-user MAC wiretap channel with one helper; $K = 3$ and $m = 2$. Here, we define $V_i \triangleq \{V_{ij} : j = 1, 2, 3, j \neq i\}$ for $i = 1, 2$.

By Lemma 3, for any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(m(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P to meet the average power constraint, then

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\beta P^{\delta}\right) \tag{91}$$

for some constant $\beta > 0$ (independent of P), where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1. This means that we can have $\Pr[\mathbf{V} \neq \hat{\mathbf{V}}] \to 0$ as $P \to \infty$.

By Fano's inequality and the Markov chain $\mathbf{V} \to Y_1 \to \hat{\mathbf{V}}$, we know that

$$\begin{aligned} H(\mathbf{V}|Y_1) &\leq H(\mathbf{V}|\hat{\mathbf{V}}) && (92)\\ &\leq 1 + \exp\left(-\beta P^{\delta}\right)\log(2Q+1)^{m(K-1)} && (93)\\ &= o(\log P) && (94) \end{aligned}$$

where $o(\cdot)$ is the little-o function. This means that

$$\begin{aligned} I(\mathbf{V}; Y_1) &= H(\mathbf{V}) - H(\mathbf{V}|Y_1) && (95)\\ &= \log(2Q+1)^{m(K-1)} - H(\mathbf{V}|Y_1) && (96)\\ &\geq \log(2Q+1)^{m(K-1)} - o(\log P) && (97) \end{aligned}$$

On the other hand, we can bound the second term in (90) as

$$\begin{aligned} I(\mathbf{V}; Y_2) &\leq I(\mathbf{V}; Y_2 - N_2) && (98)\\ &= \sum_{j=1}^{K} H\left(U_j + \sum_{i=1, i\neq j}^{m} V_{ij}\right) - H(U_1, \ldots, U_K) && (99)\\ &\leq K \log \frac{2KQ+1}{2Q+1} && (100)\\ &\leq K \log K && (101)\\ &= o(\log P) && (102) \end{aligned}$$

where (100) is due to the fact that entropy of each $U_j + \sum_{i=1,i\neq j}^{m} V_{ij}$ is maximized by the uniform distribution which takes values over a set of cardinality $2KQ+1$.

Combining (97) and (102), we obtain

$$\begin{aligned} \sup \sum_{i=1}^{m} R_i &\geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) && (103)\\ &\geq \log(2Q+1)^{m(K-1)} - o(\log P) && (104)\\ &= \frac{m(K-1)(1-\delta)}{m(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (105) \end{aligned}$$

By choosing δ arbitrarily small, we can achieve the sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ for almost all channel gains, which implies that the s.d.o.f. tuple of

$$\Bigg(\underbrace{\frac{(K-1)}{m(K-1)+1}, \ldots, \frac{(K-1)}{m(K-1)+1}}_{m \text{ item(s)}}, \underbrace{0, \ldots, 0}_{(K-m) \text{ item(s)}}\Bigg) \tag{106}$$

is achievable by symmetry, which is (83). ■

V. s.d.o.f. Region of K-User IC With Secrecy Constraints

In this section, we study the K-user IC with secrecy constraints defined in Section II-B and prove the s.d.o.f. region stated in Theorem 2. To this end, we consider both IC-CM and IC-EE and their combination IC-CM-EE in a unified framework. We first illustrate the regions for $K = 2, 3, 4$ cases as examples. The purpose of presenting $K = 4$ as an example is to show that, unlike the MAC case, starting with $K = 4$ interference constraints become effective and binding. We then provide converses separately for IC-EE and IC-CM in Section V-A and Section V-B, respectively, which imply a converse for IC-CM-EE. Finally, we show the achievability for IC-CM-EE, which implies the achievability for IC-EE and IC-CM. Specifically, we investigate the converse region in terms of its extreme points in Section V-C and show the general achievability in Section V-D.

For $K = 2$, the s.d.o.f. region in Theorem 2 becomes

$$D = \Big\{\mathbf{d} : 2d_1 + d_2 \le 1,\quad d_1 + 2d_2 \le 1,\quad d_1, d_2 \ge 0\Big\} \tag{107}$$

which is the same as (39), and is shown in Fig. 4. Note that (15) is not necessary for the two-user case, since summing the bounds $2d_1 + d_2 \le 1$ and $d_1 + 2d_2 \le 1$ up gives a new bound

$$d_1 + d_2 \le \frac{2}{3} \tag{108}$$

which is the result in Theorem 2 and makes the constraint in (15) strictly loose.

In order to provide the achievability, it suffices to check that the extreme points $(0, 0)$, $(\frac{1}{2}, 0)$, $(0, \frac{1}{2})$, and $(\frac{1}{3}, \frac{1}{3})$ are achievable. In fact the achievabilities of $(\frac{1}{2}, 0)$, $(0, \frac{1}{2})$ are similar to [36] and [46] and will be shown in Section V-C. The achievability of $(\frac{1}{3}, \frac{1}{3})$ was proved in [47] and [48]. Note that $(\frac{1}{3}, \frac{1}{3})$ is the only sum s.d.o.f. optimum point.

For $K = 3$, the s.d.o.f. region in Theorem 2 becomes

$$D = \Big\{\mathbf{d} : 3d_1 + d_2 + d_3 \le 2,\quad d_1 + 3d_2 + d_3 \le 2,\quad d_1 + d_2 + 3d_3 \le 2,\quad d_1, d_2, d_3 \ge 0\Big\} \tag{109}$$

and (15) is not necessary for the three-user case, either. This is because, due to the positiveness of each element in $\mathbf{d}$, from the first two inequalities in (109), we have

$$3d_1 + d_2 \le 3d_1 + d_2 + d_3 \le 2 \tag{110}$$

$$d_1 + 3d_2 \le d_1 + 3d_2 + d_3 \le 2 \tag{111}$$

Summing the left hand sides up of (110) and (111) gives us

$$d_1 + d_2 \le 1 \tag{112}$$

which is (15) with $V = \{1, 2\}$, and we have (15) for free from (109).

The extreme points of this region are:

$$\begin{aligned}
&\Big(0, 0, 0\Big)\\
&\Big(\frac{2}{3}, 0, 0\Big), \Big(0, \frac{2}{3}, 0\Big), \Big(0, 0, \frac{2}{3}\Big)\\
&\Big(\frac{1}{2}, \frac{1}{2}, 0\Big), \Big(\frac{1}{2}, 0, \frac{1}{2}\Big), \Big(0, \frac{1}{2}, \frac{1}{2}\Big)\\
&\Big(\frac{2}{5}, \frac{2}{5}, \frac{2}{5}\Big)
\end{aligned} \tag{113}$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers [36], [46] and Section V-C), the maximum sum of pair of s.d.o.f. (proved in Section V-C), and the maximum sum s.d.o.f. (see three-user Gaussian IC-CM-EE in [47] and [48]). Note that, $(\frac{1}{2}, \frac{1}{2})$ is the maximum sum d.o.f. for a two-user IC *without* secrecy constraints, and $(\frac{2}{5}, \frac{2}{5}, \frac{2}{5})$ is the only sum s.d.o.f. optimum point. Finally, note the difference of the extreme points of the 3-user IC in (113) from the corresponding 3-user MAC in (41), even though the s.d.o.f. regions and the extreme points of the 2-user IC and 2-user MAC in (107) and (39) were the same.

For $K = 4$, the s.d.o.f. region in Theorem 2 becomes

$$\begin{aligned}
D = \Big\{\mathbf{d} : 4d_1 + d_2 + d_3 + d_4 &\le 3,\\
d_1 + 4d_2 + d_3 + d_4 &\le 3,\\
d_1 + d_2 + 4d_3 + d_4 &\le 3,\\
d_1 + d_2 + d_3 + 4d_4 &\le 3,\\
d_1 + d_2 &\le 1,\\
d_1 + d_3 &\le 1,\\
d_1 + d_4 &\le 1,\\
d_2 + d_3 &\le 1,\\
d_2 + d_4 &\le 1,\\
d_3 + d_4 &\le 1,\\
d_1, d_2, d_3, d_4 &\ge 0\Big\}
\end{aligned} \tag{114}$$

The extreme points of this region are:

$$\begin{aligned}
&\Big(0, 0, 0, 0\Big)\\
&\Big(\frac{3}{4}, 0, 0, 0\Big), \Big(0, \frac{3}{4}, 0, 0\Big), \Big(0, 0, \frac{3}{4}, 0\Big), \Big(0, 0, 0, \frac{3}{4}\Big)\\
&\Big(\frac{2}{3}, \frac{1}{3}, 0, 0\Big) \quad \text{up to element reordering}\\
&\Big(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0\Big), \Big(\frac{1}{2}, \frac{1}{2}, 0, \frac{1}{2}\Big), \Big(\frac{1}{2}, 0, \frac{1}{2}, \frac{1}{2}\Big), \Big(0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\Big)\\
&\Big(\frac{3}{7}, \frac{3}{7}, \frac{3}{7}, \frac{3}{7}\Big)
\end{aligned} \tag{115}$$

Here, in contrast to the two-user and three-user cases, (15) is absolutely necessary. For example, the point $(\frac{3}{5}, \frac{3}{5}, 0, 0)$ satisfies (14), but not (15). In fact, it cannot be achieved, and (15) is strictly needed to enforce that fact.

Regarding the region in Theorem 2, as illustrated in the examples above, we provide a few general comments here:

1) Although (15) only states the constraints for all pairs of rates, due to the same argument in [44], it can equivalently be stated as $\sum_{i \in V} d_i \le \frac{|V|}{2}$ for all $|V| \ge 2$. We note that, when $|V| = K$, the corresponding upper bound is strictly loose due to Theorem 1 in [47] and [48], and that is why such bounds were not needed in [47] and [48], where sum s.d.o.f. was characterized.
2) As shown in the examples, when $K = 2$ or 3, (15) is not necessary. When $K \ge 4$, we need both (14) and (15) to completely characterize the region D. Neither of them can be removed from the theorem. For example, the all $\frac{1}{2}$ vector, $(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$, satisfies (15), but not (14). On the other hand, the point $(\frac{K-1}{K+1}, \frac{K-1}{K+1}, 0, 0, \ldots, 0)$, which has only two non-zero elements, satisfies (14), but not (15) for any $K \ge 4$. Therefore, (15) emerges only when $K \ge 4$. To the best of our knowledge, this is the first time that $K = 2$ or $K = 3$ do not represent the full generality of a multi-user problem, and we need to go up to $K = 4$

for this phenomenon to appear. An intuitive explanation for this phenomenon is given in the next comment.

3) Different portions of the region D are governed by different upper bounds. To see this, we can study the structure of the extreme points of D, since D is the convex hull of them. The sum s.d.o.f. tuple, which is symmetric and has no zero elements, is governed by the upper bounds in (14) due to secrecy constraints. However, as will be shown in Theorem 8 in Section V-C, all other extreme points have zeros as some elements, and therefore are governed by the upper bounds in (15) due to interference constraints in [43] and [44]. An explanation can be provided as follows: When some transmitters do not have messages to transmit, we may employ them as "helpers". Even though secrecy constraint is considered in our problem, with the help of the "helpers", the effect due to the existence of the eavesdropper in the network can be *eliminated*. Hence, this portion of the s.d.o.f. region is dominated by the interference constraints.

A. Converse for K-User IC-EE

The constraint in (15) follows from the non-secrecy constraints on the K-user IC in [43] and [44]. We note that this same constraint is valid for the converse proof of IC-CM in the next section as well.

In order to prove (14) in Theorem 2, we start with a multi-user version of the secrecy penalty lemma:

$$n\sum_{j=1}^{K} R_j \le \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Z}) + nc_{10} \tag{116}$$

$$\le \sum_{j=1, j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_{11} \tag{117}$$

for any $i = 1, \ldots, K$. Then, we apply the role of a helper lemma, Lemma 2, by treating the signal from transmitter j as the unintended noise to its neighboring transmitter-receiver pair $j-1$, i.e., for any $i = 1, \ldots, K$,

$$n\sum_{j=1}^{K} R_j \le \sum_{j=1, j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_{11} \tag{118}$$

$$\begin{aligned}\le [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + \cdots \\ + \left[h(\mathbf{Y}_{i-2}) - nR_{i-2}\right] + [h(\mathbf{Y}_i) - nR_i] + \cdots \\ + \left[h(\mathbf{Y}_{K-1}) - nR_{K-1}\right] + nc_{12}\end{aligned} \tag{119}$$

By noting that $h(\mathbf{Y}_j) \le \frac{n}{2}\log P + nc'_j$ for each j, we have

$$2n\sum_{j=1}^{K} R_j \le (K-1)\frac{n}{2}\log P + nR_i + nc_{13} \tag{120}$$

Therefore, we have a total of K bounds for $i = 1, \ldots, K$. Summing these K bounds, we obtained:

$$(2K-1)n\sum_{j=1}^{K} R_j \le K(K-1)\frac{n}{2}\log P + nc_{14} \tag{121}$$

which gave

$$D_{s,\Sigma} \le \frac{K(K-1)}{2K-1} \tag{122}$$

completing the converse proof for the sum s.d.o.f. of IC-EE in [48] (also Corollary 2 in this paper).

Here, we continue from (117) and re-interpret it as:

$$n\sum_{j=1}^{K} R_j \le \sum_{j=1, j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_{15} \tag{123}$$

$$\le \underbrace{[h(\mathbf{Y}_i) - nR_i] + \cdots + [h(\mathbf{Y}_i) - nR_i]}_{K-1 \text{ items}} + nc_{16} \tag{124}$$

$$= (K-1)h(\mathbf{Y}_i) - (K-1)nR_i + nc_{16} \tag{125}$$

$$\le (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_i + nc_{17} \tag{126}$$

where $i \in \{1, \ldots, K\}$ is arbitrary. Here, the second inequality means that we apply Lemma 2 by treating the signal from all transmitters $j \neq i$ as the unintended noise to the transmitter-receiver pair i.

Rearranging the terms in (126), dividing both sides by $\frac{n}{2}\log P$, and taking the limit $P \to \infty$ on both sides, we obtain

$$Kd_i + \sum_{j=1, j\neq i}^{K} d_j \le K-1, \qquad i = 1, \ldots, K \tag{127}$$

which is (14) in Theorem 2, completing the converse proof for IC-EE.

B. Converse for K-User IC-CM

Similarly, in order to prove (14) in Theorem 2 for K-User IC-CM, we start with a multi-user version of the secrecy penalty lemma:

$$n\sum_{j=1, j\neq i}^{K} R_j \le \textstyle\sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_i) + nc_{18} \tag{128}$$

where we focus on the secrecy constraint (13) at a single receiver, say i, as an eavesdropper, and start with the sum rate corresponding to all unintended messages at receiver i.

For the sum s.d.o.f. of IC-CM, we apply Lemma 2 to (128) by treating the signal from transmitter j as the unintended noise to its neighbor transmitter-receiver pair $j+1$, i.e., for any $i = 1, \ldots, K$

$$n\sum_{j=1, j\neq i}^{K} R_j \le \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_i) + nc_{19} \tag{129}$$

$$\begin{aligned}\le \left[\sum_{j=1}^{K-1}\left[h(\mathbf{Y}_{j+1}) - nR_{j+1}\right]\right] + \left[h(\mathbf{Y}_1) - nR_1\right] \\ - h(\mathbf{Y}_i) + nc_{20}\end{aligned} \tag{130}$$

$$= \sum_{j=1}^{K}\left[h(\mathbf{Y}_j) - nR_j\right] - h(\mathbf{Y}_i) + nc_{20} \tag{131}$$

By noting that $h(\mathbf{Y}_j) \leq \frac{n}{2}\log P + nc'_j$ for each j, we have

$$nR_i + 2n \sum_{j=1, j\neq i}^{K} R_j \leq \textstyle\sum_{j=1,j\neq i}^{K} h(\mathbf{Y}_j) + nc_{20} \quad (132)$$

$$\leq (K-1)\tfrac{n}{2}\log P + nc_{21} \quad (133)$$

Therefore, we have a total of K bounds for $i = 1, \ldots, K$. Summing these K bounds, we obtained

$$(2K-1)n\sum_{j=1}^{K} R_j \leq K(K-1)\frac{n}{2}\log P + nc_{22} \quad (134)$$

which gave

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \quad (135)$$

completing the converse proof for the sum s.d.o.f. of IC-CM in [48] (also Corollary 2 in this paper).

Here, we continue from (128) and re-interpret it as follows: For any $i \in \{1, \ldots, K\}$, we select

$$k \triangleq \begin{cases} i-1, & \text{if } i \geq 2 \\ K, & \text{if } i = 1 \end{cases} \quad (136)$$

and then have

$$\begin{aligned} n \sum_{j=1,j\neq i}^{K} R_j &\leq \left[\sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j)\right] - h(\mathbf{Y}_i) + nc_{23} && (137)\\ &\leq h(\tilde{\mathbf{X}}_k) + \left[\sum_{j=1,j\neq k}^{K} h(\tilde{\mathbf{X}}_j)\right] - h(\mathbf{Y}_i) + nc_{24} && (138)\\ &\leq h(\mathbf{Y}_i) - nR_i + \left[\sum_{j=1,j\neq k}^{K} h(\tilde{\mathbf{X}}_j)\right] - h(\mathbf{Y}_i) + nc_{25} && (139)\\ &= \left[\sum_{j=1,j\neq k}^{K} h(\tilde{\mathbf{X}}_j)\right] - nR_i + nc_{25} && (140)\\ &\leq \underbrace{[h(\mathbf{Y}_k) - nR_k] + \cdots + [h(\mathbf{Y}_k) - nR_k]}_{K-1 \text{ items}} \\ &\quad - nR_i + nc_{26} && (141)\\ &= (K-1)h(\mathbf{Y}_k) - (K-1)nR_k - nR_i + nc_{26} && (142)\\ &\leq (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_k - nR_i + nc_{26} && (143) \end{aligned}$$

which is

$$(K-1)nR_k + n\sum_{j=1}^{K} R_j \leq (K-1)\left(\frac{n}{2}\log P\right) + nc_{26} \quad (144)$$

Here, inequality (139) means that we apply Lemma 2 by treating the signal from transmitter k as the unintended noise to the transmitter-receiver pair i. Similarly, inequality (141) means that we apply Lemma 2 by treating the signal from transmitter $j \neq k$ as the unintended noise to the transmitter-receiver pair k.

Rearranging the terms in (144), dividing both sides by $\frac{n}{2}\log P$, and taking the limit $P \to \infty$ on both sides, we obtain

$$Kd_k + \sum_{j=1,j\neq k}^{K} d_j \leq K-1, \qquad k = 1, \ldots, K \quad (145)$$

which is (14) in Theorem 2, completing the converse proof for IC-CM.

C. Polytope Structure and Extreme Points

Similar to the discussion and approach in the MAC problem in Section IV-B, it is easy to see that the region D characterized by Theorem 2 is a polytope, which is equal to the convex combinations of all extreme points of D due to Theorem 4. Therefore, in order to show the tightness of region D, it suffices to prove that all extreme points of D are achievable.

We first assume that $K \geq 3$, and determine the structure of all extreme points of D in the following theorem.

Theorem 8: For the K-dimensional region D, $K \geq 3$, in Theorem 2, any extreme point must be a point with one of the following structures:

$$(0, 0, \ldots, 0), \quad (146)$$

$$\Bigg(\frac{K-1-p}{K-p}, \underbrace{\frac{1}{K-p}, \ldots, \frac{1}{K-p}}_{p \text{ items}}, \underbrace{0, \ldots, 0}_{m \text{ items}}\Bigg),$$
$$K-2 \geq p \geq 0, \quad m = K-1-p \geq 1 \quad (147)$$

$$\Bigg(\underbrace{\frac{1}{2}, \ldots, \frac{1}{2}}_{p' \text{ items}}, \underbrace{0, \ldots, 0}_{m' \text{ items}}\Bigg),$$
$$K-2 \geq p' \geq 3, \quad m' \geq 1, \quad p'+m' = K \geq 5 \quad (148)$$

$$\left(\frac{K-1}{2K-1}, \frac{K-1}{2K-1}, \ldots, \frac{K-1}{2K-1}\right) \quad (149)$$

up to element reordering.

The proof of Theorem 8 is provided in Appendix A.

Now, in order to show the tightness of region D, it suffices to show the achievability for each structure in Theorem 8. Clearly, the zero vector in (146) is trivially achievable. The symmetric tuple in (149) is achievable due to [47] and [48]. Therefore, it remains to show the achievability of the structures in (147) and (148).

In order to address the achievabilities of (147) and (148), we formulate a new channel model as a $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers. The formal definition of this channel model is given in Section V-D. Then, we have the following theorem.

Theorem 9: For the $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers, as far as $p \geq 0$, $m \geq 1$, and N is finite, the following s.d.o.f. tuple is achievable:

$$\Bigg(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}\Bigg) \quad (150)$$

for almost all channel gains.

The proof of Theorem 9 is provided in Section V-D.

Here, we provide a few comments about Theorem 9. Theorem 9 provides quite general results, and subsumes some other known cases:

1) The result in [36] is a special case of Theorem 9 with $p = 0, m \geq 1, N = 1$.
2) (147) is a special case of Theorem 9 with $p \geq 0$, $m = K - 1 - p \geq 1, N = m + 1$.
3) (148) is a byproduct of Theorem 9: By choosing $p = p' - 1, m = 1, N = m' + 1$, we know that with just one helper, the following s.d.o.f. tuple is achievable:
$$\Big(\underbrace{\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}}_{p' \text{ items}}, 0\Big) \tag{151}$$
Now, if we add $m' - 1$ more independent helpers into the network, (148) can be achieved trivially.

Therefore, with the help of Theorem 9, each structure in Theorem 8 can be achieved, which provides the achievability proof for Theorem 2 for $K \geq 3$.

Finally, we address the $K = 2$ case. In this case, the region D characterized by (14)-(16) in Theorem 2 is given by (107). In order to provide the achievability, it suffices to prove that the extreme points $(\frac{1}{2}, 0), (0, \frac{1}{2})$, and $(\frac{1}{3}, \frac{1}{3})$ are achievable. The achievability of $(\frac{1}{3}, \frac{1}{3})$ was proved in [47] and [48]. The achievabilities of $(\frac{1}{2}, 0), (0, \frac{1}{2})$ are the special cases of Theorem 9 with $p = 0, m = 1, N = 2$.

D. Achievability

The $(p + 1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers is
$$Y_i = \sum_{j=1}^{p+1+m} h_{ji} X_j + N_i, \qquad i = 1, \ldots, p+1 \tag{152}$$
$$Z_k = \sum_{j=1}^{p+1+m} g_{jk} X_j + N_{z_k}, \qquad k = 1, \ldots, N \tag{153}$$
where Y_i is the channel output of receiver i, Z_k is the channel output of external eavesdropper k, X_j is the channel input of transmitter j, h_{ji} is the channel gain of the jth transmitter to the ith receiver, g_{jk} is the channel gain of the jth transmitter to the kth eavesdropper, and $\{N_1, \ldots, N_{p+1}, N_{z_1}, \ldots, N_{z_N}\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All the channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_{ji} and g_{jk} are non-zero. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_j^2\right] \leq P$, for $j = 1, \ldots, p + 1 + m$.

Transmitter j, $j = p + 2, \ldots, p + 1 + m$, is an independent helper in the network. On the other hand, each transmitter i, $i = 1, \ldots, p + 1$, has a message W_i intended for the receiver Y_i. A rate tuple $(R_1, \ldots, R_{p+1})$ is said to be achievable if for any $\epsilon > 0$, there exist joint n-length codes such that each receiver i can decode the corresponding message reliably, i.e., the probability of decoding error is less than ϵ for all messages,
$$\max_i \Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon \tag{154}$$
where $\hat{W}_i$ is the estimation based on its observation $\mathbf{Y}_i$. The secrecy constraints are defined as follows:
$$\frac{1}{n} H(W_{-i}^{p+1} | \mathbf{Y}_i) \geq \frac{1}{n} H(W_{-i}^{p+1}) - \epsilon \tag{155}$$
$$\frac{1}{n} H(W_1, \ldots, W_{p+1} | \mathbf{Z}_k) \geq \frac{1}{n} H(W_1, \ldots, W_{p+1}) - \epsilon \tag{156}$$
where $i = 1, \ldots, p + 1$, $k = 1, \ldots, N$, $W_{-i}^{p+1} \triangleq \{W_1, \ldots, W_{p+1}\} \backslash \{W_i\}$. A s.d.o.f. tuple, $(d_1, \ldots, d_{p+1})$, is achievable if there exists an achievable rate tuple $(R_1, \ldots, R_{p+1})$ such that
$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P} \tag{157}$$
for $i = 1, \ldots, p + 1$.

Now, we prove Theorem 9, i.e., for $p \geq 0$, $m \geq 1$, and N is finite, the following s.d.o.f. tuple is achievable:
$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}\Big) \tag{158}$$
for almost all channel gains.

The purpose of Theorem 9 is to prove the achievability of the structure (147) in Theorem 8. As shown in (147), we partition the transmitters into three groups: 1) the first group consists of only one transmitter with the largest s.d.o.f., $\frac{K-1-p}{K-p}$, which is no smaller than $\frac{1}{2}$, 2) the second group consists of $p \geq 0$ transmitters with the same s.d.o.f., $\frac{1}{K-p}$, which is no larger than $\frac{1}{2}$, and 3) the third group consists of $m \geq 1$ transmitters serving as independent helpers. Therefore, in (158), we consider the $(p+1)$-user IC with m helpers where $K = p + 1 + m$. Therefore, (158) and Theorem 9 show the achievability of (147). We know from remark 2) above that the achievability of (148) is a byproduct of Theorem 9. Also, (146) is trivially achieved, and the achievability of (149) is shown in [47] and [48]. Therefore, we focus on Theorem 9, from this point on.

The technique we use in the proof of Theorem 9 is asymptotical interference alignment [49] and cooperative jamming [14] with structured signals. The alignment scheme is illustrated in Fig. 7 with $m = 3, p = 2, N = 1$. In Fig. 7, we partition the transmitters into three groups, which are $\{X_1\}$ as the first group, $p = 2$ other transmitters $\{X_2, X_3\}$ as the second group, and $m = 3$ helpers as the third group. From the perspective of Y_1 and the eavesdropper Z, due to the existence of independent helpers, the alignment signaling design is similar to that in wiretap channel with helpers in [36, Fig. 4]. However, from the perspective of Y_2, Y_3, and the eavesdropper Z, the alignment signaling design is similar to that in the interference channel in [47, Fig. 2] (see the details of the corresponding design in [48]). This suggests that the signalling scheme that achieves on arbitrary extreme point of the s.d.o.f. region is in between the signalling scheme that achieves the sum s.d.o.f. of IC-CM-EE in [47] and [48] and the signalling scheme used in the helper network in [36]. Furthermore, if we let $p = 0$, the signaling scheme in Fig. 7 would be almost identical to [36, Fig. 4].

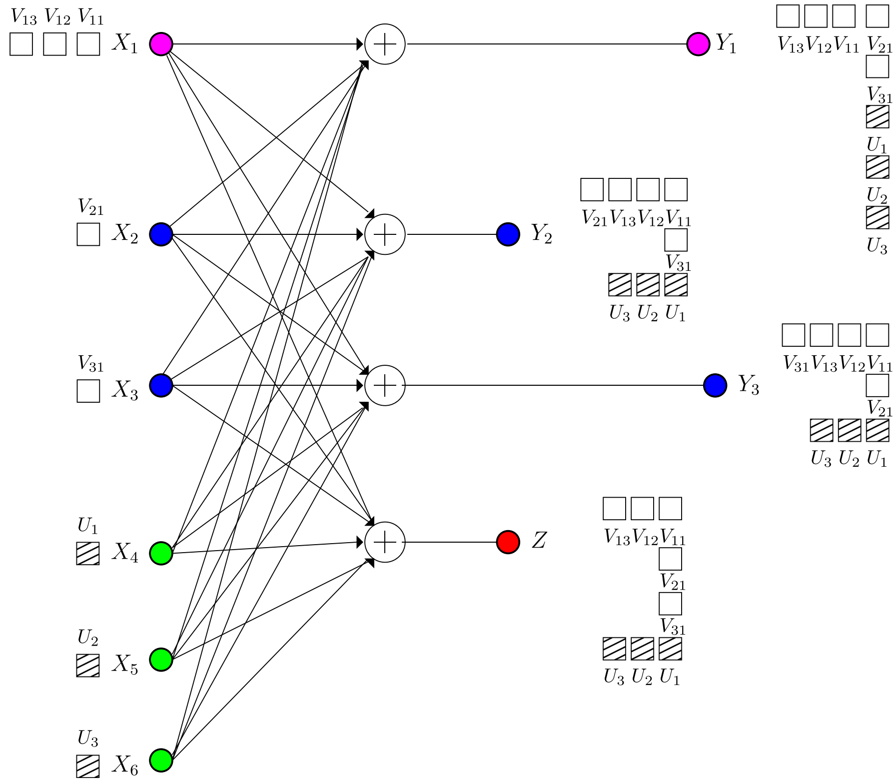

Fig. 7. Illustration of secure interference alignment of Theorem 9 with $m = 3$, $p = 2$, $N = 1$.

However, we cannot let m be equal to 0. As far as the number of independent helper(s) in Fig. 7, m, is non-zero, in contrast to the scheme in [47, Fig. 2], the legitimate transmitters in the first and second groups do not send cooperative jamming signals by themselves, however, in [47] and [48] for IC-CM-EE without helpers, each legitimate transmitter needed to send both message signals and a cooperative signal. Note that in Fig. 7 here, legitimate transmitters $\{X_1, X_2, X_3\}$ do not send any cooperative jamming signals (no shaded boxes).

Here, we give the general achievable scheme. Let l be a large constant. Let us define a set T_1 which will represent *dimensions* as follows:

$$T_1 \triangleq \left\{ \left(\prod_{(j,k)\in L} h_{jk}^{r_{jk}}\right)\left(\prod_{k=1}^{N}\prod_{j=1}^{p+1+m} g_{jk}^{s_{jk}}\right) : r_{jk}, s_{jk} \in \{1,\ldots,l\}\right\} \tag{159}$$

where L contains almost all pairs corresponding to the cross-link channel gains

$$L = \Big\{(j,k) : j \in \{2,\ldots,p+2\}, k = 1\Big\} \cup \Big\{(j,k) : j \in \{1,\ldots,p+1+m\}, k \in \{2,\ldots,p+1\}, j \neq k\Big\} \tag{160}$$

Clearly, starting from the second helper X_{p+3}, if there exists any, the cross-link channel gains to the first legitimate receiver Y_1 are not in the set L. Therefore, we define the sets $\{T_j\}_{j=2}^{m}$

$$T_j = \frac{1}{h_{p+1+j,1}} T_1, \qquad j = 2,\ldots,m \tag{161}$$

Let M_i be the cardinality of T_i, $i = 1,\ldots,m$. Note that all M_i are the same, thus we denote them as M,

$$M \triangleq l^{|L|+N(p+1+m)} = l^{\theta} \tag{162}$$

where $\theta \triangleq (p+1+m)p + p + N(p+1+m) + 1$.

Let $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ be the vector containing all the elements in the set T_j for any possible i. Therefore, $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ are M-dimensional vectors containing M rationally independent real numbers in T_j. The sets $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ will represent the *dimensions* along which message signals are transmitted. In particular, as illustrated in Fig. 7, for each legitimate transmitter i, $i = 1,\ldots,p+1$, the message signal V_{i1} is transmitted in dimensions $\mathbf{t}_{i1}$. In order to asymptotically align U_1 from the first helper X_{p+2} with all V_{i1}s, the cooperative jamming signal U_1 is transmitted in dimensions $\mathbf{t}_{(1)}$. Similarly, for the first transmitter X_1, the message signal V_{1j}, $j = 2,\ldots,m$, is transmitted in dimensions $\mathbf{t}_{1j}$. Since we want to align the cooperative jamming signal U_j from the helper X_{p+1+j} with V_{1j} one by one, the jamming signal U_j is transmitted in dimensions $\mathbf{t}_{(j)}$.

Let us define an mM dimensional vector $\mathbf{b}_1$ by stacking $\mathbf{t}_{i1}$s as

$$\mathbf{b}_1^T = \left[\mathbf{t}_{11}^T, \mathbf{t}_{12}^T, \ldots, \mathbf{t}_{1m}^T\right] \tag{163}$$

Then, transmitter 1 generates a vector $\mathbf{a}_1$, which contains a total of mM discrete signals each identically and independently drawn from $C(a, Q)$ given in (24). For convenience, we partition this transmitted signal as

$$\mathbf{a}_1^T = \left[\mathbf{v}_{11}^T, \mathbf{v}_{12}^T, \ldots, \mathbf{v}_{1m}^T\right] \tag{164}$$

where $\mathbf{v}_{1j}$ represents the information symbols in V_{1j}. Each of these vectors has length M, and therefore, the total length of $\mathbf{a}_1$ is mM. The channel input of transmitter 1 is

$$x_1 = \mathbf{a}_1^T \mathbf{b}_1 \tag{165}$$

Similarly, for the second group transmitters X_i, $i = 2, \ldots, p+1$, let $\mathbf{b}_i$ be $\mathbf{b}_i = \mathbf{t}_{i1}$. Then, transmitter i generates a vector $\mathbf{a}_i = \mathbf{v}_{i1}$, which contains a total of M discrete signals each identically and independently drawn from $C(a, Q)$ given in (24). The channel input of transmitter i is

$$x_i = \mathbf{a}_i^T \mathbf{b}_i = \mathbf{v}_{i1}^T \mathbf{t}_{i1}, \qquad i = 2, \ldots, p+1 \tag{166}$$

Finally, for the third group transmitters X_k, $k = p+2, \ldots, p+1+m$, serving as the helpers, let $\mathbf{b}_k$ be $\mathbf{b}_k = \mathbf{t}_{(k-p-1)}$. Then, helper k generates a vector $\mathbf{u}_{k-p-1}$ representing the cooperative jamming signal in U_{k-p-1}, which contains a total of M discrete signals each identically and independently drawn from $C(a, Q)$ given in (24). The channel input of transmitter k is

$$x_k = \mathbf{u}_{k-p-1}^T \mathbf{b}_k = \mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)} \tag{167}$$

where $k = p+2, \ldots, p+1+m$.

Before we investigate the performance of this signalling scheme, we analyze the structure of the received signals at the receivers. To see the detailed dimension structure of the received signals at the receivers, let us define $\tilde{T}_i$ as a superset of T_i, as follows

$$\tilde{T}_1 \triangleq \left\{ \left(\prod_{(j,k)\in L} h_{jk}^{r_{jk}} \right) \left(\prod_{k=1}^{N} \prod_{j=1}^{p+1+m} g_{jk}^{s_{jk}} \right) : \right.$$
$$\left. r_{jk}, s_{jk} \in \{1, \ldots, l+1\} \right\} \tag{168}$$

$$\tilde{T}_j = \frac{1}{h_{p+1+j,1}} \tilde{T}_1, \qquad j = 2, 3, \ldots, m \tag{169}$$

where L is defined in (160) and the cardinalities of all T_i sets are the same and are denoted as $\tilde{M} = (l+1)^\theta$. Also, it is easy to check that since pair $(p+1+j, 1) \notin L$ for $j \geq 2$, we must have

$$\tilde{T}_i \cap \tilde{T}_j = \phi \tag{170}$$

for all $i \neq j$.

We first focus on receiver 1, which has the channel output

$$y_1 = \sum_{i=1}^{p+1+m} h_{i1} x_1 + n_1 \tag{171}$$

Substituting (165), (166) and (167) into (171), we get

$$y_1 = h_{11} x_1 + \sum_{j=2}^{p+1} h_{j1} x_j + \sum_{k=p+2}^{p+1+m} h_{k1} x_k + n_1 \tag{172}$$

$$= h_{11} \left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i} \right) + \left(\sum_{j=2}^{p+1} h_{j1} \mathbf{v}_{j1}^T \mathbf{t}_{j1} \right)$$
$$+ \left(\sum_{k=p+2}^{p+1+m} h_{k1} \mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)} \right) + n_1 \tag{173}$$

$$= \left(\mathbf{v}_{11}^T h_{11} \mathbf{t}_{11} \right) + \left(\mathbf{v}_{12}^T h_{11} \mathbf{t}_{12} \right) + \ldots + \left(\mathbf{v}_{1m}^T h_{11} \mathbf{t}_{1m} \right)$$
$$+ \left(\sum_{j=2}^{p+1} h_{j1} \mathbf{v}_{j1}^T \mathbf{t}_{j1} + \sum_{k=p+2}^{p+1+m} h_{k1} \mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)} \right) + n_1 \tag{174}$$

Since $\mathbf{v}_{ij}$ and $\mathbf{u}_{k-p-1}$ are integer signals in $C(a, Q)$, it suffices to study their dimensions. In addition, note that $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ represent the same dimensions in T_j defined in (159) and (161). It is easy to verify that

$$h_{j1} T_1 \subseteq \tilde{T}_1, \qquad j = 2, \ldots, p+1 \tag{175}$$

$$h_{k1} T_{k-p-1} \subseteq \tilde{T}_1, \qquad k = p+2, \ldots, p+1+m \tag{176}$$

which implies that except the intended message signals $\mathbf{v}_{1i}$, $i = 1, \ldots, m$, all unintended signals including message signals and cooperative jamming signals are all transmitted in the dimensions belonging to $\tilde{T}_1$. On the other hand, for intended signals,

$$h_{11} T_1 \subset h_{11} \tilde{T}_1 \tag{177}$$

$$h_{11} T_i \subseteq h_{11} \tilde{T}_i = \frac{h_{11}}{h_{p+1+i,1}} \tilde{T}_1, \qquad i = 2, \ldots, m \tag{178}$$

Note that the pair $(p+1+i, 1) \notin L$ for $i \geq 2$ which implies that

$$h_{11} \tilde{T}_i \cap h_{11} \tilde{T}_j = \phi \tag{179}$$

for all $i, j \in \{1, \ldots, m\}$, $i \neq j$. Furthermore, $(1, 1) \notin L$ either, which implies that

$$h_{11} \tilde{T}_i \cap \tilde{T}_1 = \phi, \qquad i \in \{1, \ldots, m\} \tag{180}$$

Together with (179), this indicates that the dimensions are separable as suggested by the parentheses in (174) and also the Y_1 side of Fig. 7, which further implies that all the elements in the set

$$R_1 \triangleq \left(\bigcup_{j=1}^{m} h_{11} \tilde{T}_j \right) \cup \tilde{T}_1 \tag{181}$$

are rationally independent, and thereby the cardinality of R_1 is

$$M_R \triangleq |R_1| = (m+1)\tilde{M} = (m+1)(l+1)^\theta \tag{182}$$

For the legitimate receivers Y_i, $i = 2, \ldots, p+1$, without loss of generality, we focus on receiver 2; by symmetry, a similar structure will exist at all other receivers. We observe that

$$y_2 = h_{12}x_1 + \sum_{j=2}^{p+1} h_{j2}x_j + \sum_{k=p+2}^{p+1+m} h_{k2}x_k + n_2 \tag{183}$$

$$= h_{12}\left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i}\right) + \left(\sum_{j=2}^{p+1} h_{j2}\mathbf{v}_{j1}^T \mathbf{t}_{j1}\right) + \left(\sum_{k=p+2}^{p+1+m} h_{k2}\mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)}\right) + n_2 \tag{184}$$

$$= \left(h_{22}\mathbf{v}_{21}^T \mathbf{t}_{21}\right) + \left(\mathbf{v}_{11}^T h_{12}\mathbf{t}_{11} + \sum_{j=3}^{p+1} \mathbf{v}_{j1}^T h_{j2}\mathbf{t}_{j1} + \mathbf{u}_1^T h_{p+2,2}\mathbf{t}_{(1)}\right) + \left(\mathbf{v}_{12}^T h_{12}\mathbf{t}_{12} + \mathbf{u}_2^T h_{p+3,2}\mathbf{t}_{(2)}\right) + \ldots + \left(\mathbf{v}_{1m}^T h_{12}\mathbf{t}_{1m} + \mathbf{u}_m^T h_{p+1+m,2}\mathbf{t}_{(m)}\right) + n_2 \tag{185}$$

Similarly, we observe that in the second set of parentheses of (185), since $\mathbf{t}_{i1}$ and $\mathbf{t}_{(1)}$ represent the same dimensions in T_1 for all i, we have

$$h_{i2}T_1 \subseteq \tilde{T}_1, \qquad i \in \{1, \ldots, p+2\}, i \neq 2 \tag{186}$$

Starting from the third set of parentheses of (185), we have

$$h_{12}T_j \subseteq \tilde{T}_j \tag{187}$$

$$h_{p+1+j,2}T_j \subseteq \tilde{T}_j \tag{188}$$

for all $j = 2, \ldots, m$. In addition, since the pair $(2, 2) \notin L$, we can infer that

$$h_{22}T_1 \subseteq h_{22}\tilde{T}_1 \tag{189}$$

and

$$h_{22}\tilde{T}_1 \cap \tilde{T}_j = \phi \tag{190}$$

for $j = 1, \ldots, m$. Together with (170), this indicates that the dimensions are separable as suggested by the parentheses in (185) and also the Y_2 side of Fig. 7, which further implies that all the elements in the set

$$R_2 \triangleq \left(\bigcup_{j=1}^{m} \tilde{T}_j\right) \cup h_{22}\tilde{T}_1 \tag{191}$$

are rationally independent, and thereby the cardinality of R_2 is M_R in (182).

For the external eavesdropper Z_k, we note that

$$z_k = g_{1k}x_1 + \sum_{j=2}^{p+1} g_{jk}x_j + \sum_{i=p+2}^{p+1+m} g_{ik}x_i + n_{z_k} \tag{192}$$

$$= g_{1k}\left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i}\right) + \left(\sum_{j=2}^{p+1} g_{jk}\mathbf{v}_{j1}^T \mathbf{t}_{j1}\right) + \left(\sum_{i=p+2}^{p+1+m} g_{ik}\mathbf{u}_{i-p-1}^T \mathbf{t}_{(i-p-1)}\right) + n_{z_k} \tag{193}$$

$$= \left(\mathbf{v}_{11}^T g_{1k}\mathbf{t}_{11} + \sum_{j=2}^{p+1} \mathbf{v}_{j1}^T g_{jk}\mathbf{t}_{j1} + \mathbf{u}_1^T g_{p+2,k}\mathbf{t}_{(1)}\right) + \left(\mathbf{v}_{12}^T g_{1k}\mathbf{t}_{12} + \mathbf{u}_2^T g_{p+3,k}\mathbf{t}_{(2)}\right) + \ldots + \left(\mathbf{v}_{1m}^T g_{1k}\mathbf{t}_{1m} + \mathbf{u}_m^T g_{p+1+m,k}\mathbf{t}_{(m)}\right) + n_{z_k} \tag{194}$$

In the first set of parentheses of (194), since $\mathbf{t}_{i1}$ and $\mathbf{t}_{(1)}$ represent the same dimensions in T_1 for all i, we have

$$g_{ik}T_1 \subseteq \tilde{T}_1, \qquad i \in \{1, \ldots, p+2\} \tag{195}$$

Starting from the second set of parentheses of (194), we have

$$g_{1k}T_j \subseteq \tilde{T}_j \tag{196}$$

$$g_{p+1+j,k}T_j \subseteq \tilde{T}_j \tag{197}$$

for all $j = 2, \ldots, m$. Due to (170), this indicates that the dimensions are separable as suggested by the parentheses in (194) and also the Z side of Fig. 7, which further implies that all the elements in the set

$$R_Z \triangleq \left(\bigcup_{j=1}^{m} \tilde{T}_j\right) \tag{198}$$

are rationally independent, and thereby the cardinality of R_Z is M_{R_Z}

$$M_{R_Z} \triangleq |R_Z| = m\tilde{M} = m(l+1)^\theta \tag{199}$$

We will compute the secrecy rates achievable with the asymptotic alignment based scheme proposed above by using the following theorem.

Theorem 10 ([48, Th. 2]): For K'-user interference channels with confidential messages, the following rate region is achievable

$$R_i \geq I(V_i; Y_i) - \max_{j \in \mathcal{K}'_{-i}} I(V_i; Y'_j | V_{-i}^{K'}), \qquad i = 1, \ldots, K' \tag{200}$$

where $V_{-i}^{K'} \triangleq \{V_j\}_{j=1, j\neq i}^{K'}$ and $\mathcal{K}'_{-i} = \{1, \ldots, i-1, i+1, \ldots, K'\}$. The auxiliary random variables $\{V_i\}_{i=1}^{K'}$ are mutually independent, and for each i, we have the following Markov chain $V_i \to X'_i \to (Y'_1, \ldots, Y'_{K'})$.

We can reinterpret Theorem 10 as follows: For the $(p+1)$-user IC-CM-EE with m helpers and N external eavesdroppers, since each independent helper's contribution is the same as noise to both items in (200), which depend only on marginal distributions, we can treat the $(p+1)$-user IC-CM-EE channel as a $(p+1+N)$-user IC-CM with N new transmitters which keep silent, i.e., V_i and X'_i, $i = p+2, \ldots, p+1+N$, are equal to zero, and

$$p(y'_1, \ldots, y'_{p+1+N} | x'_1, \ldots, x'_{p+1+N}) = p(y_1, \ldots, y_{p+1}, z_1, \ldots, z_N | x_1, \ldots, x_{p+1}) \quad (201)$$

where x' and y' are the transmitter and receiver of the $(p+1+N)$-user IC-CM and x, y, z are the entities of the original $(p+1)$-user IC-CM-EE with m helpers and N external eavesdropper.

We thereby first select V_i as

$$V_1 \stackrel{\triangle}{=} \mathbf{a}_1 \quad (202)$$
$$V_i \stackrel{\triangle}{=} \mathbf{v}_{i1}, \qquad i = 2, \ldots, p+1 \quad (203)$$

where $\mathbf{a}_1$ is defined in (164). Then, we evaluate the (200) for $i = 1, \ldots, p+1$.

For $i = 1$, by Lemma 3, for any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M_R+\delta)}}$ and $a = \frac{\gamma_1 P^{\frac{1}{2}}}{Q}$, the probability of error of estimating V_1 as $\tilde{V}_1$ based on Y_1 can be upper bounded by

$$\Pr(e_1) \leq \exp\left(-\eta_{\gamma_1} P^{\delta}\right) \quad (204)$$

Furthermore, by Fano's inequality, we can conclude that

$$\begin{aligned} I(V_1; Y_1) &\leq I(V_1; \tilde{V}_1) && (205)\\ &= H(V_1) - H(V_1|\tilde{V}_1) && (206)\\ &\geq \frac{mM(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (207)\\ &= \frac{m(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta} + \frac{\delta}{l^{\theta}}}\left(\frac{1}{2}\log P\right) + o(\log P) && (208) \end{aligned}$$

where $o(\cdot)$ is the little-o function. This provides a lower bound for the first term in (200) with $i = 1$.

Next, we need to derive an upper bound for the second item in (200), i.e, the secrecy penalty, for $i = 1$. For and $j \in \{2, \ldots, p+1\}$, by the Markov chain,

$$V_1 \to \left(\sum_{k=1}^{p+1} h_{kj} X_{kj}, V_2^{p+1}\right) \to Y_j \quad (209)$$

we have

$$\begin{aligned} I(V_1; Y_j|V_2^{p+1}) &\leq I\left(V_1; \sum_{k=1}^{p+1} h_{kj} X_k \middle| V_2^{p+1}\right) && (210)\\ &= H\left(\sum_{k=1}^{p+1} h_{kj} X_k \middle| V_2^{p+1}\right) - H\left(\sum_{k=1}^{p+1} h_{kj} X_k \middle| V_1^{p+1}\right) && (211) \end{aligned}$$

The first term in (211) can be rewritten as

$$H\left(\sum_{k=1}^{p+1} h_{kj} X_k \middle| V_2^{p+1}\right) = H\left[\sum_{i=k}^{m}\left(\mathbf{v}_{1k}^T h_{1j}\mathbf{t}_{1k} + \mathbf{u}_k^T h_{p+1+k,j}\mathbf{t}_{(k)}\right)\right] \quad (212)$$

Note that there are in total mM_R rational dimensions each taking value from $C(a, 2Q)$. Regardless of the distribution in each rational dimension, the entropy is maximized by uniform distribution, i.e.,

$$\begin{aligned} H\left(\sum_{k=1}^{p+1} h_{kj} X_k \middle| V_2^{p+1}\right) &\leq \log\left[(2Q+1)^{m\tilde{M}}\right] && (213)\\ &= \frac{m\tilde{M}(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (214) \end{aligned}$$

The second term in (211) is

$$\begin{aligned} H\left(\sum_{k=1}^{p+1} h_{kj} X_k \middle| V_1^{p+1}\right) &= H\left[\sum_{i=k}^{m}\left(\mathbf{u}_k^T h_{p+1+k,j}\mathbf{t}_{(k)}\right)\right] && (215)\\ &= \log\left[(2Q+1)^{mM}\right] && (216)\\ &= \frac{mM(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (217) \end{aligned}$$

Substituting (214) and (217) into (211), we get

$$I(V_1; Y_j|V_2^{p+1}) \leq \frac{m(\tilde{M}-M)(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (218)$$

We note that

$$\begin{aligned} \xi &\stackrel{\triangle}{=} \frac{m(\tilde{M}-M)(1-\delta)}{M_R+\delta} && (219)\\ &= \frac{m(\tilde{M}-M)(1-\delta)}{(m+1)\tilde{M}+\delta} && (220)\\ &= \frac{m\left[(l+1)^{\theta} - l^{\theta}\right](1-\delta)}{(m+1)(l+1)^{\theta}+\delta} && (221)\\ &= \frac{m\left[\sum_{k=0}^{\theta-1}\binom{\theta}{k} l^k\right](1-\delta)}{(m+1)(l+1)^{\theta}+\delta} && (222) \end{aligned}$$

The maximum power of l in the numerator is $\theta - 1$ and is less than the power θ of l in the denominator. This implies that when m and δ are fixed, by choosing l large enough, the factor before the $\frac{1}{2}\log P$ term in (218), ξ, can be made arbitrarily small. Due to the non-perfect (i.e., only asymptotical) alignment, the upper bound for the information leakage rate is not a constant as in [46], but a function which can be made to approach zero d.o.f.

Similarly, we can derive the following

$$I(V_1; Z_k|V_2^{p+1}) \leq \xi\left(\tfrac{1}{2}\log P\right) + o(\log P) \quad (223)$$

where Z_k, $k = 1, \dots, N$, is the external eavesdropper. Substituting (208), (218) and (223) into (200), we obtain a lower bound for the achievable secrecy rate R_1 as

$$R_1 \geq \left[\frac{m(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta} + \frac{\delta}{l^{\theta}}} - \xi \right] \left(\frac{1}{2} \log P \right) + o(\log P) \tag{224}$$

Similarly, it is easy to derive that

$$R_i \geq \left[\frac{(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta} + \frac{\delta}{l^{\theta}}} - \xi' \right] \left(\frac{1}{2} \log P \right) + o(\log P) \tag{225}$$

for $i = 2, \dots, p+1$ and ξ' can be made arbitrarily small. By choosing $l \to \infty$ and $\delta \to 0$, we can achieve a s.d.o.f. tuple arbitrarily close to

$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \dots, \frac{1}{m+1},}_{p \text{ items}} \Big) \tag{226}$$

which is (150), completing the proof of Theorem 9.

VI. Conclusions

In this paper, we determined the *entire s.d.o.f. regions* of K-user MAC wiretap channel, K-user IC-EE, K-user IC-CM, and K-user IC-CM-EE. The converse for MAC directly followed from the results in [45] and [46]. The converse for IC was shown to be dominated by secrecy constraints and interference constraints in different parts. To show the tightness and achieve the regions characterized by the converses, we provided a general method to investigate this class of channels, whose s.d.o.f. regions have a polytope structure. We provided an equivalence between the extreme points in the polytope structure and the rank of sub-matrices containing all active upper bounds associated with each extreme point. Then, we achieved each extreme point by relating it to a specific channel model. More specifically, the extreme points of the MAC region can be achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. On the other hand, the asymmetric extreme points of the IC region can be achieved by a $(p+1)$-user IC-CM with m helpers, and N external eavesdroppers.

Appendix A
Proof of Theorem 8

Regarding Theorem 8, first, we have few comments:

1) (148) will not be possible until $K \geq 5$ due to the constraint $K-2 \geq p' \geq 3$.
2) The point in (148) with $p' = K-1$, i.e., $(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}, 0)$, is actually an extreme point, but since (147) with $p = K-2$ also includes it, we classify it as (147) here.
3) Assume that we allow $p' = 2$ in (148) with $K \geq 5$. Then, the point becomes

$$\mathbf{d}_1 = \left(\frac{1}{2}, \frac{1}{2}, 0, 0, \dots, 0 \right) \tag{227}$$

However, this is just the middle point of two points in (147). More specifically, by choosing $p = 1$ in (147), we have $\mathbf{d}_1' = (\frac{K-2}{K-1}, \frac{1}{K-1}, 0, 0, \dots, 0)$ and $\mathbf{d}_1'' = (\frac{1}{K-1}, \frac{K-2}{K-1}, 0, 0, \dots, 0)$ (by swapping the first two elements in $\mathbf{d}_1'$). Here $\mathbf{d}_1' \neq \mathbf{d}_1''$ due to $K \geq 5$, and also it is easy to check that $\mathbf{d}_1 = \frac{1}{2}(\mathbf{d}_1' + \mathbf{d}_1'')$, which means that $\mathbf{d}_1$ is not an extreme point. Therefore, in (148) p' must satisfy $p' \geq 3$.

Now, we start the proof of Theorem 8. In order to speak of a polytope, we re-write (16) as

$$-d_i \leq 0, \qquad i = 1, \dots, K \tag{228}$$

Then, we can write all the left hand sides of (14), (15), (228) as an $\hat{N} \times K$ matrix $\mathbf{H}$ with corresponding right hand sides forming an $\hat{N}$-length column vector $\mathbf{h}$, i.e., all points $\mathbf{d}$ in D satisfy

$$\mathbf{Hd} \leq \mathbf{h} \tag{229}$$

where $\hat{N} \triangleq 2K + \binom{K}{2} = 2K + K(K-1)/2$. For any extreme point $\mathbf{d} \in D$, let $J(\mathbf{d})$ be a set such that

$$J(\mathbf{d}) = \left\{ l : \mathbf{H}_l \mathbf{d} = \mathbf{h}_l, \quad l \in \{1, \dots, \hat{N}\} \right\} \tag{230}$$

where $\mathbf{H}_l$ is the lth row of $\mathbf{H}$ and $\mathbf{h}_l$ is the lth element of $\mathbf{h}$. Therefore, $J(\mathbf{d})$ represents all active boundaries. The remaining rows satisfy

$$\mathbf{H}_l \mathbf{d} < \mathbf{h}_l \tag{231}$$

for $l \notin J$.

For convenience, denote by $\mathbf{H}_J$ the sub-matrix of $\mathbf{H}$ with rows indexed by $J \triangleq J(\mathbf{d})$. Similarly denote by $\mathbf{h}_J$ the sub-vector of $\mathbf{h}$ with rows indexed by J. In order to find all extreme points in D, by Theorem 5 in Section III-A, we need to find all $K \times (K+1)$ sub-matrices $(\mathbf{H}', \mathbf{h}')$ of $(\mathbf{H}, \mathbf{h})$ with $\text{rank}(\mathbf{H}') = K$ such that $\mathbf{Hd} \leq \mathbf{h}$ and $\mathbf{H}'\mathbf{d} = \mathbf{h}'$, which is also equivalent to finding all index sets J representing the active boundaries such that $\mathbf{Hd} \leq \mathbf{h}$, $\mathbf{H}_J \mathbf{d} = \mathbf{h}_J$, and $\text{rank}(\mathbf{H}_J) = K$.

For convenience of presentation, we always partition the set J as a union of mutually exclusive sets S, P and Z, i.e.,

$$J = S \cup P \cup Z \tag{232}$$

We denote by S the row indices representing the active boundaries in (14)

$$S \triangleq \Big\{ s_i \triangleq s(i) : \mathbf{H}_{s_i} \mathbf{d} = h_{s_i} \text{ such that } (K-1)d_i + \sum_{j=1}^{K} d_j = K-1, \quad i \in \{1, \dots, K\} \Big\} \tag{233}$$

where s_i stands for the function $s(i)$ of the coordinate i with the value as the row index of $\mathbf{H}$ corresponding to the active boundaries $(K-1)d_i + \sum_{j=1}^{K} d_j = K-1$. Thus, we have a one-to-one mapping between the row index and the function $s_i \triangleq s(i)$, i.e., if the row index $s_i \in J$, we know exactly the ith upper bound in (14) is active; on the other hand, if we know the coordinate i, we can determine the unique corresponding row index in $\mathbf{H}$ by the mapping $s : i \mapsto s_i$.

Similarly, we denote by P the row indices representing the active boundaries in (15)

$$P \triangleq \Big\{ p_V \triangleq p(V) : \mathbf{H}_{p_V}\mathbf{d} = h_{p_V} \text{ such that } \sum_{i\in V} d_i = 1, \quad V \subseteq \{1,\dots,K\}, |V| = 2 \Big\} \tag{234}$$

where the value of p_V is the corresponding row index of $\mathbf{H}$.

Finally, we denote by Z the row indices representing the active boundaries in (228)

$$Z \triangleq \Big\{ z_i \triangleq z(i) : \mathbf{H}_{z_i}\mathbf{d} = h_{z_i} \text{ such that } d_i = 0, \quad i \in \{1,\dots,K\} \Big\} \tag{235}$$

where the value of z_i is the corresponding row index of $\mathbf{H}$.

In order to find all $K \times (K+1)$ sub-matrices $(\mathbf{H}', \mathbf{h}')$ of $(\mathbf{H}, \mathbf{h})$ with $\text{rank}(\mathbf{H}') = K$ such that $\mathbf{H}'\mathbf{d} = \mathbf{h}'$, there are approximately in total

$$\binom{\hat{N}}{K} \approx \frac{\left(\frac{K+2}{2}\right)^K e^K}{\sqrt{2\pi K}} \tag{236}$$

possible selections of K equations in (229) for large K; in getting (236), we used $\hat{N} = 2K + K(K-1)/2$ and Stirling's approximation [56]. In order for this search to have a reasonable complexity, we need to investigate the structure of D more carefully. We identify the following simple properties for the extreme points in the following lemmas.

Lemma 4: Let $\mathbf{d}$ *be a non-zero extreme point in D. Then, it must satisfy the following properties:*

1) $\max_k d_k \le \frac{K-1}{K}$.

2) At most one element, if there is any, in $\mathbf{d}$ *is strictly larger than* $\frac{1}{2}$.

3) If there exists an element, say d_i, which is equal to $\frac{1}{2}$, then, $d_j \le d_i = \frac{1}{2}$ for all j.

4) If $|S| \ge 2$ and $\forall s_i, s_j \in S$, where $i \ne j$, then $0 < d_i = d_j \le \frac{1}{2}$.

5) If $s_i \in S$, then $d_j \le d_i$ for all j. Equivalently, if $|S| \ge 1$ and $s_i \in S$, then $d_i = \max_{j=1,\dots,K} d_j$. Equivalently, if $|S| \ge 1$ and $d_i = \max_{j=1,\dots,K} d_j$, then $s_i \in S$.

6) If $\max_i d_i > \frac{1}{2}$, then $|S| \le 1$.

The proof of Lemma 4 is provided in Appendix B. In addition to the properties of the elements of the extreme points, we also need some results regarding the rank of the sub-matrices. It is easy to verify that a trivial necessary condition for $\text{rank}(\mathbf{H}_J) = K$ is $|S| + |P| + |Z| \ge K$. More formally, we have the following lemma.

Lemma 5: For an extreme point $\mathbf{d}$, *rank*$(\mathbf{H}_J) = K$ *only if*

$$\mathit{rank}(\mathbf{H}_{S\cup P}) + |Z| \ge K \tag{237}$$

Lemma 6: Let $\mathbf{d}$ *be a non-zero extreme point of D. If $|P| \ge 1$ and $\max_k d_k > \frac{1}{2}$, then there exists a coordinate i_* such that*

$$\frac{K-1}{K} \ge d_{i_*} = \max_k d_k > \frac{1}{2} \tag{238}$$

and a non-empty set

$$U' \triangleq \Big\{ j : d_j = 1 - d_{i_*} > 0 \Big\} \tag{239}$$

with cardinality $m' \triangleq |U'| = |P|$ and

$$P = P' \triangleq \Big\{ p_V : V = \{i_*, j\}, j \in U' \Big\} \tag{240}$$

In addition, S is either empty or

$$S = \{s_{i_*}\} \tag{241}$$

Futhermore,

$$\mathit{rank}(\mathbf{H}_{S\cup P}) = |P| + \mathbf{1}_{\{|S|\ge 1\}} \tag{242}$$

where $\mathbf{1}_{\{\cdot\}}$ *is the indicator function.*

Lemma 7: Let $\mathbf{d}$ *be a non-zero extreme point of D. If $|P| \ge 1$ and $\max_k d_k \le \frac{1}{2}$, then there exists a non-empty set*

$$U'' = \Big\{ i : d_i = \frac{1}{2} \Big\} \tag{243}$$

with cardinality $m'' \triangleq |U''|$, $2 \le m'' \le K-1$, and

$$P = P'' \triangleq \Big\{ p_V : V = \{k, j\},\ k \ne j,\ \text{and } k, j \in U'' \Big\} \tag{244}$$

with rank

$$\mathit{rank}(\mathbf{H}_P) = \begin{cases} m'', & |P| > 1 \\ 1, & |P| = 1 \end{cases} \tag{245}$$

In addition, S is either empty or

$$S = \Big\{ s_i : i \in U'' \Big\} \tag{246}$$

Futhermore,

$$\mathit{rank}(\mathbf{H}_{S\cup P}) = \begin{cases} 1, & |P| = 1 \text{ and } |S| = 0 \\ m'' + \mathbf{1}_{\{|S|\ge 1\}}, & o.w. \end{cases} \tag{247}$$

where $\mathbf{1}_{\{\cdot\}}$ *is the indicator function.*

The proofs of Lemmas 5, 6, and 7 are provided in Appendix B.

Now, we are ready to prove Theorem 8.

Case: $|Z| = K$. Clearly, $\text{rank}(\mathbf{H}_Z) = K$ and only the zero vector satisfies

$$\mathbf{H}\mathbf{0} \le \mathbf{h} \tag{248}$$

$$\mathbf{H}_Z\mathbf{0} = \mathbf{h}_Z \tag{249}$$

Thus, $\mathbf{0}$ is an extreme point of D, which is (146). Therefore, in the remaining discussion we focus on non-zero points and $|Z| < K$.

Case: $|P| = 0$. Since $|Z| < K$, by Lemma 5, $|S| \ge 1$.

If $|S| = 1$, then again by Lemma 5, $|Z| = K-1$. By property 5) of Lemma 4, $S = \{s_i\}$ for some i and $Z = \{z_j : j \ne i\}$. The extreme point $\mathbf{d}$ has the structure (147) with $p = 0$.

If $|S| = K$, then by property 4) of Lemma 4, $Z = \phi$, and the corresponding extreme point is (149).

If $2 \le |S| \le K-1$, due the positiveness implied by property 4) of Lemma 4 and the cardinality constraint by Lemma 5, the only consistent Z, which gives a solution for $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$, is

$$Z = \Big\{ z_j : s_j \notin S \Big\} \tag{250}$$

Denote by x any d_i for $s_i \in S$. Then, we have

$$Kx + (|S| - 1)x = K - 1 \tag{251}$$

which implies that

$$x = \frac{K-1}{K-1+|S|} \tag{252}$$

Since P is empty, x must satisfy $x < \frac{1}{2}$ due to $|S| \geq 2$ and property 4) of Lemma 4. Substituting (252) into $x < \frac{1}{2}$ gives $|S| > K-1$, which contradicts the assumption $|S| < K$. Therefore, the solution given by $\mathbf{H}_J \mathbf{d} = \mathbf{h}_J$, where $J = S \cup Z$, violates (231).

Case: $|P| \geq 1$ **and** $\max_k d_k > \frac{1}{2}$. First of all, due to the positiveness implied by (238) and (239), the consistent set Z must satisfy

$$Z \subseteq \left\{ z_k : k \notin \{i_*\} \cup U' \right\} \tag{253}$$

which implies $|Z| \leq K - |U'| - 1 = K - |P| - 1$.

If S is empty, by Lemma 6, $\text{rank}(\mathbf{H}_{S\cup P}) = |P|$, which implies

$$\text{rank}(\mathbf{H}_{S\cup P}) + |Z| < K \tag{254}$$

which implies that $\text{rank}(\mathbf{H}_J) < K$, which does not give any extreme point, by Lemma 5.

Therefore, S is non-empty and determined by (241). In addition, Lemma 6 gives

$$\text{rank}(\mathbf{H}_{S\cup P}) = |P| + 1 \tag{255}$$

If $|P| = K-1$, due to (239) and (241), we have the equality in (14) hold for i_*, i.e.,

$$Kd_{i_*} + (K-1)(1-d_{i_*}) = K - 1 \tag{256}$$

which leads to $d_{i_*} = 0$ contradicting (238).

Therefore, $|P| < K-1$. Then, the consistent set Z satisfying Lemma 5 is

$$Z = \left\{ z_k : k \notin \{i_*\} \cup U' \right\} \tag{257}$$

In addition, due to (239) and (241), we have the equality in (14) hold for i_*, i.e.,

$$Kd_{i_*} + |P|(1-d_{i_*}) = K - 1 \tag{258}$$

which implies that

$$d_{i_*} = \frac{K-1-|P|}{K-|P|} \tag{259}$$

Since $d_{i_*} = \max_k d_k > \frac{1}{2}$, we have

$$|P| < K - 2 \tag{260}$$

The solution of this choice is exactly (147) with $1 \leq p < K-2$, and it satisfies (229).

Case: $|P| \geq 1$ **and** $\max_k d_k \leq \frac{1}{2}$. If S is empty, then by Lemma 7,

$$\text{rank}(\mathbf{H}_{S\cup P}) = \begin{cases} m'', & |P| > 1 \\ 1, & |P| = 1 \end{cases} \tag{261}$$

where m'' is the cardinality of U'' defined in (243). Since $m'' \geq 2$, for both cases, $\text{rank}(\mathbf{H}_{S\cup P}) \leq m''$. Due to the positiveness of the elements in U'', $|Z| \leq K - m''$. Therefore, by Lemma 5, the cardinality of Z can only take the value $|Z| = K - m''$, i.e.,

$$d_j = 0, \quad \forall j \notin U'' \tag{262}$$

Also, Lemma 5 implies that $|P| > 1$ and $m'' > 2$; otherwise, $\text{rank}(\mathbf{H}_{S\cup P}) + |Z| = 1 + |Z| \leq 1 + K - m'' \leq K - 1 < K$.

Therefore, the elements in $\mathbf{d}$ are either $\frac{1}{2}$ or 0, and the number of $\frac{1}{2}$s is m''. Note that S is empty. Therefore, for any $i \in U''$, we must have the equality in (14) not hold, i.e.,

$$\frac{K}{2} + (m''-1)\frac{1}{2} < K - 1 \tag{263}$$

which indicates that

$$m'' < K - 1 \tag{264}$$

Combining with the condition $m'' > 2$ gives an extreme point that has the structure (148).

It remains to discuss the case where S is non-empty. By Lemma 7, S is determined by (246) and

$$\text{rank}(\mathbf{H}_{S\cup P}) = m'' + 1 \tag{265}$$

If $m'' = K-1$, then the only solution is given by choosing $Z = \{z_j : j \notin U''\}$ with $|Z| = 1$, which is the structure in (147) with $p = K-2$.

If $m'' < K-1$, then $\text{rank}(\mathbf{H}_{S\cup P}) < K$. By Lemma 5 and the positiveness implied by U'' with cardinality m'', Z must satisfy

$$K - m'' \geq |Z| \geq K - \text{rank}(\mathbf{H}_{S\cup P}) = K - m'' - 1 > 0 \tag{266}$$

i.e., Z is not empty and the extreme point $\mathbf{d}$ has either $K - m'' - 1$ or $K - m''$ zero(s). On the other hand, $\mathbf{d}$ also has in total m'' $\frac{1}{2}$s due to the definition of U'' in (243). If $|Z| = K - m''$, then the extreme point $\mathbf{d}$ has the following form

$$d_i = \begin{cases} \frac{1}{2}, & i \in U'' \\ 0, & i \notin U'' \end{cases} \tag{267}$$

and we must have the equality in (14) hold for some $i \in U''$, i.e.,

$$\frac{K}{2} + (m''-1)\frac{1}{2} = K - 1 \tag{268}$$

which is not valid since $m'' < K-1$. Therefore, the equations corresponding to the selection of J are inconsistent. On the other hand, if $|Z| = K - m'' - 1$, then the extreme point $\mathbf{d}$ has the following form

$$d_i = \begin{cases} \frac{1}{2}, & i \in U'' \\ 0, & z_i \in Z \\ x, & \text{o.w.} \end{cases} \tag{269}$$

where $0 < x < \frac{1}{2}$. Again, we must have the equality in (14) hold for some $i \in U''$, i.e.,

$$\frac{K}{2} + (m''-1)\frac{1}{2} + x = K - 1 \tag{270}$$

which implies that

$$x = \frac{K-1-m''}{2} \tag{271}$$

Substituting this formula into $0 < x < \frac{1}{2}$ leads to

$$K-2 < m'' < K-1 \tag{272}$$

which is not possible since m'' is an integer, which completes the proof of Theorem 8.

Appendix B
Proofs of Lemma 4 Through 7

A. Proof of Lemma 4

We prove all the properties one by one.

1) The constraint (14) and the positiveness constraint in (16) imply that for any coordinate i, we have

$$Kd_i \le Kd_i + \sum_{j\ne i} d_j = K-1 \tag{273}$$

i.e., $d_i \le \frac{K-1}{K}$ for any i. Therefore, $\max_k d_k \le \frac{K-1}{K}$.

2) We prove by contradiction. Assume that we have distinct coordinates, i, j, such that $d_i, d_j > \frac{1}{2}$ in $\mathbf{d}$. Then, the set $V \triangleq \{i, j\}$ with $|V| = 2$ violates the constraint in (15). Therefore, this contradiction implies that at most one element, if any, in $\mathbf{d}$ is strictly larger than $\frac{1}{2}$.

3) Similarly, assume that there exists a j such that $d_j > \frac{1}{2}$. Since $d_i = \frac{1}{2}$ by assumption, $d_i + d_j > 1$, which violates constraint (15). This implies that $d_j \le d_i = \frac{1}{2}$ for all j.

4) Let $i, j \in S$ and $i \ne j$. Due to the definition of S, $s_i, s_j \in S$, i.e., from (233)

$$Kd_i + d_j + \sum_{k=1,k\ne i,j}^{K} d_k = K-1 \tag{274}$$

$$Kd_j + d_i + \sum_{k=1,k\ne i,j}^{K} d_k = K-1 \tag{275}$$

which implies $(K-1)d_i = (K-1)d_j$. Since $K-1 > 0$, $d_i = d_j$. Furthermore, due to property 2), both are no larger than $\frac{1}{2}$, and due to property 3), for any k, $d_k \le d_i$. If $d_i = 0$, then the point $\mathbf{d}$ is the zero vector, which contradicts the assumption that $\mathbf{d}$ is a non-zero extreme point in D. Therefore, $d_i = d_j > 0$.

5) The three equivalent statements in this property are simply from three different perspectives addressing the same fact that the coordinates of $\mathbf{d}$, which are associated with the elements in S, are the *most significant* coordinates, whose corresponding elements have the maximum value in $\mathbf{d}$. We will prove the first statement and then prove the equivalence of all three statements.

We prove the first statement of property 5) by contraction. Assume that there exists a j such that $d_j > d_i$. Then, consider the following expression (for $K \ge 3$)

$$\begin{aligned} Kd_j + d_i + \sum_{k=1,k\ne i,j}^{K} d_k &= d_j + d_i + (K-1)d_j + \sum_{k=1,k\ne i,j}^{K} d_k && (276)\\ &> d_j + d_i + (K-1)d_i + \sum_{k=1,k\ne i,j}^{K} d_k && (277)\\ &= Kd_i + \sum_{k=1,k\ne i}^{K} d_k && (278)\\ &= K-1 && (279)\end{aligned}$$

where the last equality is due to the assumption $s_i \in S$. This result violates the constraint (14). Therefore, for all j, $d_j \le d_i$.

Next, we prove the second statement of property 5) using the first statement. This is trivially true because the assumption $|S| \ge 1$ and $s_i \in S$ imply that, by the first statement, $d_i \ge d_j$ for all j, i.e., $d_i = \max_j d_j$.

Then, we prove the third statement of property 5) using the second statement. By assumption, let $d_i = \max_k d_k$. However, assume that $s_i \notin S$. This implies that there exists another coordinate j, $j \ne i$ such that $s_j \in S$ (since $|S| \ge 1$) and thereby by the second statement $d_j = \max_k d_k = d_i$. Then, consider

$$Kd_i + d_j + \sum_{k=1,k\ne i,j}^{K} d_k = Kd_j + d_i + \sum_{k=1,k\ne i,j}^{K} d_k = K-1 \tag{280}$$

where the last equality is due to $s_j \in S$. This implies that s_i must belong to S by definition in (233), i.e., $s_i \in S$, which contradicts the assumption that $s_i \notin S$.

Finally, we prove the first statement of property 5) using the third statement. We prove this by contradiction as well. As stated in the condition of the first statement, $s_i \in S$, this means $|S| \ge 1$. Assume that there exists at least one element which is strictly larger than d_i. Choose the largest one among them and denote it by d_j. Clearly, $j \ne i$ and $d_j = \max_k d_k > d_i$. By the third statement, $s_j \in S$. Then, $|S| \ge 2$ and by property 4) $d_i = d_j$, which contradicts the assumption $d_j > d_i$.

6) We prove $|S| \le 1$ by contraction. Assume that $|S| \ge 2$. Due to property 4) and the second statement of property 5), we have two distinct $j, k \in S$ such that $\frac{1}{2} \ge d_j = d_k = \max_i d_i > \frac{1}{2}$, which leads to a contradiction. Thus, $|S| \le 1$.

B. Proof of Lemma 5

It is straightforward that

$$\text{rank}(\mathbf{H}_Z) = |Z| \tag{281}$$

since there are in total $|Z|$ 1s in the sub-matrix $\mathbf{H}_Z$ and the row index and column index of any two 1s are different. Since $(S \cup P) \cap Z = \phi$, we have

$$\begin{aligned} K &= \text{rank}(\mathbf{H}_J) = \text{rank}(\mathbf{H}_{S\cup P\cup Z}) && (282)\\ &\le \text{rank}(\mathbf{H}_{S\cup P}) + \text{rank}(\mathbf{H}_Z) && (283)\end{aligned}$$

C. Proof of Lemma 6

If $|P| = 1$, then $P = \{p_V\}$ for a unique $V = \{i, j\}$ with $|V| = 2$. If $d_i = d_j$, then $d_i = d_j = \frac{1}{2}$ and $\max_k d_k \leq \frac{1}{2}$ due to property 3) of Lemma 4, which contradicts the condition $\max_k d_k > \frac{1}{2}$. Therefore, $d_i \neq d_j$. Without loss of generality, let $d_i > d_j$, then $d_i > \frac{1}{2}$ and i is the i_* required in Lemma 6 due to property 2) of Lemma 4. By property 1) of Lemma 4, $d_j = 1 - d_{i_*} > 0$, thus $j \in U'$. If there exists any k, $k \neq j$, such that $d_k = 1 - d_{i_*}$, then clearly $V' \stackrel{\triangle}{=} \{i_*, k\} \neq V$, but $p_{V'} \in P$, which contradicts the condition $|P| = 1$. Hence, $U' = \{j\}$ and P satisfies (240).

If $|P| \geq 2$, assume that $V_1 = \{i, j\}$, $V_2 = \{x, y\}$, $V_1 \neq V_2$, and $p_{V_1}, p_{V_2} \in P$. Without loss of generality, let $d_i = \max_{k\in\{i,j,x,y\}} d_k$. If $d_i < \frac{1}{2}$, then $d_j + d_i < 1$, which contradicts $p_{V_1} \in P$. If $d_i = \frac{1}{2}$, then due to property 3) of Lemma 4, $\max_k d_k \leq \frac{1}{2}$, which contradicts the condition $\max_k d_k > \frac{1}{2}$. Therefore, $d_i = \max_{k\in\{i,j,x,y\}} d_k > \frac{1}{2}$ and i is the i_* required in Lemma 6. For any $p_V \in P$, let $V = \{a, b\}$ and assume $d_a \geq d_b$. If $d_a = \frac{1}{2}$, this leads to a contradiction of $d_{i_*} > \frac{1}{2}$ due to property 3) of Lemma 4. Thus, $d_a > \frac{1}{2}$. Due to property 2) of Lemma 4, the coordinate a must be i_*, i.e., $a = i_*$. Then, $d_b = 1 - d_{i_*} > 0$ and that is true for any p_V. Hence, $|P| = |U'|$ and (240) are trivially true.

If S is empty, we have a sub-matrix which has the form (by removing all columns containing all zeros and rearranging the columns)

$$\mathbf{H}_{S\cup P} = \mathbf{H}_P \doteq \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 \end{bmatrix} \tag{284}$$

where the number of rows is $|P| = |U'|$, the number of columns is $|P| + 1$, and the index of the first column corresponds to i_* and the indices of other columns correspond to U' defined in (239). Therefore, $\text{rank}(\mathbf{H}_{S\cup P}) = |P|$ and the proof is completed.

If S is not empty, due to (238) and property 6) of Lemma 4, $|S| = 1$. Furthermore, due to property 5) of Lemma 4, $s_{i_*} \in S$, which is (241). Note that $\mathbf{H}_S$ is a K-length row vector containing no zeros. If $|P|+1 < K$, then $\mathbf{H}_S$ has more columns than the sub-matrix on the right hand side of (284). $\mathbf{H}_{S\cup P} = |P| + 1$ is true. If $|P| + 1 = K$, then

$$\mathbf{H}_{P\cup S} = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 \\ K & 1 & 1 & 1 & \dots & 1 \end{bmatrix} \stackrel{\triangle}{=} M(K) \tag{285}$$

where $M(n)$ is $n \times n$ square matrix as in (285), where $n \geq 2$. Therefore, $\mathbf{H}_{P\cup S} = M(K)$. If we denote $f(n) \stackrel{\triangle}{=} \det[M(n)]$, then it is easy to write the recursive formula as

$$f(n) = (-1)^n - f(n-1), \qquad n \geq 3 \tag{286}$$

$$f(2) = 1 - K \tag{287}$$

which gives that $f(n) = (-1)^n(n - K - 1)$, i.e., $\det \mathbf{H}_{P\cup S} = \det M(K) = (-1)^{K+1} \neq 0$ and $\text{rank}(\mathbf{H}_{P\cup S}) = |P| + 1 = K$, which completes the proof.

D. Proof of Lemma 7

If $\max_k d_K < \frac{1}{2}$, then $|P| = 0$, which contradicts the assumption $|P| \geq 1$. Therefore, $\max_k d_K = \frac{1}{2}$, which implies $|U''| \geq 1$. Assume that $i_* \in U''$. Due to property 3) of Lemma 4, $d_j \leq d_{i_*} = \frac{1}{2}$ for all j. If $\max_{k\neq i_*} d_k < \frac{1}{2}$, then we cannot find a set V such that $|V| = 2$ and $\sum_{k\in V} d_k = 1$, i.e., $|P| = 0$, which contradicts the assumption $|P| \geq 1$. Thus, $m'' \stackrel{\triangle}{=} |U''| \geq 2$. On the other hand, if $m'' = K$, by definition of U'', all elements in $\mathbf{d}$ are $\frac{1}{2}$, which violates the constraint (14). Therefore, $m'' \leq K - 1$.

Next, P'' defined in (244) satisfies $P'' \subseteq P$. On the other hand, for any coordinate pair (k', j') such that $k' \neq j'$ and $p_{\{k',j'\}} \in P$, since $d_{k'}, d_{j'} \leq \frac{1}{2}$, we must have $d_{k'} = d_{j'} = \frac{1}{2}$, and by definition of U'', $k', j' \in U''$, which implies $p_{\{k',j'\}} \in P''$. Therefore, $P = P''$.

If S is empty, then $\mathbf{H}_P = 1$ if $|P| = 1$ and the proof is completed. If S is empty but $|P| > 1$, the index set of the columns of $\mathbf{H}_P$, which contains nonzero elements, is U'' due to (244). Therefore, $\text{rank}(\mathbf{H}_P) \leq |U''| = m''$. In order to study the rank, we remove the columns containing all zeros and rearrange the columns. Assume that

$$U'' = \left\{i_1, i_2, \dots, i_{m''}\right\} \tag{288}$$

where $i_1 = i_*$. Then, consider a $m'' \times m''$ sub-matrix of $\mathbf{H}_P$

$$\mathbf{H}_{J''} \doteq \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \end{bmatrix} \tag{289}$$

where

$$J'' \stackrel{\triangle}{=} \{p_V : V = \{i_*, i_j\}, j = 2, \dots, m''\} \cup \{p_{\{i_2,i_3\}}\} \subseteq P \tag{290}$$

It is easy to verify that $\det \mathbf{H}_{J''} = (-1)^{m''} \times 2 \neq 0$, therefore $\text{rank}(\mathbf{H}_{J''}) = m''$, i.e., $\text{rank}(\mathbf{H}_P) = m''$. This completes the proof of the case where S is empty.

Assume that $|S| \geq 1$, by property 5) of Lemma 4, S must have the form of (246). If $|P| = 1$, $m'' = |U''| = 2$. Then, the $3 \times K$ matrix $\mathbf{H}_{P\cup S}$ must have the structure

$$\mathbf{H}_{P\cup S} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ K & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & K & 1 & 1 & 1 & \dots & 1 \end{bmatrix} \tag{291}$$

where the indices of the first two columns belong to U''. Clearly, $\mathbf{H}_{P\cup S} = 3 = m'' + 1$ since $m'' = 2$.

If $|P| > 1$, by using the J'' in (290) and the condition $m'' \leq K-1$, we have

$$\mathbf{H}_{J'' \cup S} = \left[\begin{array}{ccccccc|cccc} 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \hline K & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & K & 1 & 1 & \dots & 1 & 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & K & 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & K & 1 & 1 & \dots & 1 \end{array}\right] \quad (292)$$

Due to [57, Sec. 2.2, Problem 7],

$$\text{rank}(\mathbf{H}_{P \cup S}) = \text{rank}(\mathbf{H}_{J'' \cup S}) = \text{rank}(\mathbf{H}_{J''}) + 1 = m'' + 1 \quad (293)$$

which completes the proof.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[5] R. Liu, I. Maric, P. Spasojevic, 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.

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

[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secure broadcasting: The secrecy rate region," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008, pp. 834–841.

[9] E. Ekrem and S. Ulukus, "On secure broadcasting," in *Proc. 42nd Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Oct. 2008, pp. 676–680.

[10] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Mar. 2009, Art. ID 824235.

[11] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *Proc. 43rd Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2009, pp. 318–323.

[12] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[13] 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.

[14] 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.

[15] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wire-tap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008, pp. 1014–1021.

[16] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[17] S. Ulukus and E. Ekrem, "Cooperative secrecy in wireless communications," in *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds. New York, NY, USA: Springer-Verlag, 2009.

[18] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 389–393.

[19] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inf. Theory*, submitted. [Online]. Available: http://arxiv.org/abs/cs/0611125

[20] 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.

[21] M. Yuksel and E. A. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2007, pp. 13–18.

[22] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *Proc. IEEE Inf. Theory Workshop*, Porto, Portugal, May 2008, pp. 154–158.

[23] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[24] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[25] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Mar. 2009, Art. ID 142374.

[26] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012.

[27] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *Proc. IEEE Inf. Theory Workshop Netw. Inf. Theory*, Volos, Greece, Jun. 2009, pp. 336–340.

[28] X. He, "Cooperation and information theoretic security in wireless networks," Ph.D. dissertation, Dept. Elect. Eng., Pennsylvania State Univ., State College, PA, USA, 2010.

[29] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," *IEEE Trans. Inf. Theory*, submitted. [Online]. Available: http://arxiv.org/abs/1003.0729

[30] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

[31] 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.

[32] J. Xie and S. Ulukus, "Real interference alignment for the K-user Gaussian interference compound wiretap channel," in *Proc. 48th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2010, pp. 1252–1257.

[33] 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.

[34] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008, pp. 826–833.

[35] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

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

[37] J. Xie and S. Ulukus, "Sum secure degrees of freedom of two-unicast layered wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1931–1943, Sep. 2013.

[38] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568–1571, Aug. 2013.

[39] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. 47th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2013, pp. 1–5.

[40] M. Nafea and A. Yener, "How many antennas does a cooperative jammer need for achieving the degrees of freedom of multiple antenna Gaussian channels in the presence of an eavesdropper?" in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Oct. 2013, pp. 774–780.

[41] M. Nafea and A. A. Yener, "Degrees of freedom of the single antenna Gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Austin, TX, USA, Dec. 2013, pp. 273–276.

[42] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley, 2006.

[43] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, SA, Australia, Sep. 2005, pp. 2065–2069.
[44] 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.
[45] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, Jul. 2013, pp. 1337–1341.
[46] 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.
[47] J. Xie and S. Ulukus, "Unified secure DoF analysis of K-user Gaussian interference channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, Jul. 2013, pp. 1107–1111.
[48] 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.
[49] 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.
[50] A. S. Motahari, S. O. Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *IEEE Trans. Inf. Theory*, submitted. [Online]. Available: http://arxiv.org/abs/0908.1208
[51] D. N. C. Tse and S. V. Hanly, "Multiaccess fading channels—Part I. Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, Nov. 1998.
[52] B. Grünbaum, *Convex Polytopes*, 2nd ed. New York, NY, USA: Springer-Verlag, 2003.
[53] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.
[54] M. Padberg, *Linear Optimization and Extensions*, 2nd ed. New York, NY, USA: Springer-Verlag, 1999.
[55] R. H. Etkin and E. Ordentlich, "The degrees-of-freedom of the K-user Gaussian interference channel is discontinuous at rational channel coefficients," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4932–4946, Nov. 2009.
[56] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.
[57] F. Zhang, *Matrix Theory: Basic Results and Techniques*, 2nd ed. New York, NY, USA: Springer-Verlag, 2011.

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'14) 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 her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communications, information theory, signal processing, networking, information theoretic physical layer security, and energy harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010-2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY (2007-2010) and IEEE TRANSACTIONS ON COMMUNICATIONS (2003-2007). She served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on wireless communications powered by energy harvesting and wireless energy transfer (2015), *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks (2012), IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks (2011), IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the 2014 IEEE PIMRC, Communication Theory Symposium at 2014 IEEE Globecom, Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007-2009.