Secure Degrees of Freedom Region of the Gaussian Interference Channel with Secrecy Constraints

Jianwei Xie Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu *ulukus@umd.edu*

Abstract*—The sum secure degrees of freedom (s.d.o.f.) of the K-user interference channel (IC) with secrecy constraints has been determined recently as $\frac{K(K-1)}{2K-1}$ [1], [2]. In this paper, we determine the entire s.d.o.f. region of this channel model. The converse includes constraints both due to secrecy as well as due to interference. 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 4-user case, i.e., the 2 or 3-user cases do not illustrate the generality of the problem. In order to prove the achievability, we use the polytope structure of the converse region. The extreme points of the converse 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.

I. Introduction

Information-theoretic security of communication was first considered by Shannon in [3] 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 [4]. 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 [5]. Leung-Yan-Cheong and Hellman extended Wyner's setting to a Gaussian channel, which is degraded [6]. This line of research has been extended to many multi-user scenarios, for both general and Gaussian channel models, see e.g., [7]–[11]. The secrecy capacity regions of most 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, see e.g., [1], [2], [12]–[17]. In this paper, we focus on the K-user Gaussian interference channel (IC) with secrecy constraints. The secrecy capacity region of the IC remains open. The *sum* s.d.o.f. has been determined as $\frac{K(K-1)}{2K-1}$ in [1], [2]. Here, we determine the *entire s.d.o.f. region* of the K-user IC. The entire s.d.o.f. region of the multiple access (MAC) wiretap channel has been determined recently in [18].

We consider the IC with three different secrecy constraints in a unified framework (see Fig. 1) as in [1], [2]: 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 [1], [2] by using the *secrecy penalty* lemma and the *role of a helper* lemma [17] 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 [1], [2] is based on asymptotical real interference alignment [19] to enable simultaneous alignment at multiple receivers.

In order to develop a converse for the *entire region* for the IC case, we start by re-examining the converse proof in [1], [2] for the sum s.d.o.f. We note that the original steps used 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 IC case, there are many different ways in which the *role of a helper* lemma can be invoked as there are multiple receivers. In the IC, by pairing up helpers (interferers) and the receivers we obtain $(K-1)^K$ upper bounds. 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, we do not apply the *next one* (i.e., $k=i-1$ and $k=i+1$) selection of helpers/interferers as we have done in [1, Eqns. (24) and (45)]. Instead, we choose all of the transmitters as interfering with a single transmitter-receiver pair; see (12) and (21) 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 [20], [21] as additional upper bounds. We note that such upper bounds are not binding for the IC sum s.d.o.f. converses. In fact, such non-secrecy upper

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

bounds for the IC are not binding even 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 most generality of the problem, and we need to study $K = 4$ to observe a certain multi-user phenomenon to take effect.

The converse region for the IC with secrecy constraints has a *polytope* structure. Polytope is a bounded polyhedron, which is an intersection of a finite number of half-spaces. In order to show the achievability of the polytope region, we use Minkowski theorem [22, Theorem 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. For the IC, 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, we develop an achievable scheme for each extreme point. In particular, each extreme point of the converse region is achieved by a $(K-m)$-user IC-CM with m helpers and N independent external eavesdroppers, for $m \geq 1$ and finite N. Finally, as a byproduct, 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.

II. System Model, Definitions and the Result

K-user Gaussian IC with secrecy constraints (Fig. 1) is:

$$Y_i = \sum_{j=1}^{K} h_{ji} X_j + N_i, \qquad i = 1, \dots, K \tag{1}$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \tag{2}$$

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 $\{N_1, \dots, N_K, N_Z\}$ 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 $i = 1, \dots, K$.

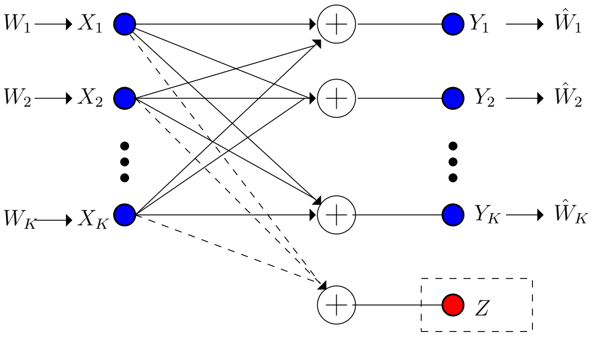

Fig. 1. K-user interference channel (IC) with secrecy constraints.

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 $R_i \overset{\triangle}{=} \frac{1}{n} \log |\mathcal{W}_i|$, 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 $\mathbf{X}_i \overset{\triangle}{=} X_i^n$ is the n-length channel input of user i. The legitimate receiver j decodes the message as $\hat{W}_j$ based on its observation $\mathbf{Y}_j$, where $\mathbf{Y}_j \overset{\triangle}{=} Y_j^n$. A secrecy rate tuple $(R_1, \dots, R_K)$ 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,

$$\max_j \Pr\left[W_j \neq \hat{W}_j\right] \leq \epsilon \tag{3}$$

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

1) In IC-EE, all of the messages are kept information-theoretically secure against the external eavesdropper,

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

where $\mathbf{Z} \overset{\triangle}{=} Z^n$.

2) In IC-CM, all unintended messages are kept information-theoretically secure against each receiver,

$$\frac{1}{n} H(W_{-i}^K | \mathbf{Y}_i) \geq \frac{1}{n} H(W_{-i}^K) - \epsilon, \quad i = 1, \dots, K \tag{5}$$

where $W_{-i}^K \overset{\triangle}{=} \{W_1, \dots, W_{i-1}, W_{i+1}, \dots, W_K\}$.

3) In IC-CM-EE, 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 (4) and (5).

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

$$D = \Big\{ \mathbf{d} : (R_1, \dots, R_K) \text{ is achievable} \\ \text{and } d_i \overset{\triangle}{=} \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P}, \ i = 1, \dots, K \Big\} \tag{6}$$

The sum s.d.o.f. is defined as the largest sum of d_i in D.

The sum s.d.o.f. of the K-user IC-EE, IC-CM, and IC-CM-EE is characterized in the following theorem.

Theorem 1 ([1, Theorem 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.*

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*

$$Kd_i + \sum_{j=1,j\neq i}^{K} d_j \leq K-1, \qquad i=1,\ldots,K \tag{7}$$

$$\sum_{i\in V} d_i \leq 1, \qquad \forall\, V \subseteq \{1,\ldots,K\},\ |V|=2 \tag{8}$$

$$d_i \geq 0, \qquad i=1,\ldots,K \tag{9}$$

for almost all channel gains.

III. Preliminaries

A. Polytope Structure and Extreme 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: $\text{Co}(X) \triangleq \{\sum_i \lambda_i \mathbf{x}_i \mid \mathbf{x}_i \in X,\ \sum_i \lambda_i = 1,\ \lambda_i \in R, \text{ and } \lambda_i \geq 0,\ \forall i\}$. 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 $P = \{\mathbf{x} \in R^n \mid \mathbf{Hx} \leq \mathbf{h}\}$. A set $P \subseteq R^n$ is a *polytope* if there is a finite set $X \subseteq R^n$ such that $P = \text{Co}(X)$. Then, we have the following theorem.

Theorem 3 ([22, Theorem 3.1.3]) *Let $P \subseteq R^n$. Then, P is a bounded polyhedron if only if P is a polytope.*

Therefore, if $P \subseteq R^n$ is a polytope, then it is a convex hull of some finite set X. 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. 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.*

Theorem 4 (Minkowski, 1910. [22, Theorem 2.4.5]) *Let $P \subseteq R^n$ be a compact convex set. Then,*

$$P = Co(Ex(P)). \tag{10}$$

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 ([23, Theorem 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$(\mathbf{H}') = n$.*

IV. Converse for K-User IC-EE

The constraint in (8) follows from the non-secrecy constraints on the K-user IC in [20], [21]. 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 (7) in Theorem 2, we re-examine [1, Eqn. (23)]. Originally, we applied [16, Lemma 2] in [1] by treating the signal from transmitter j as the unintended noise to its neighboring transmitter-receiver pair $j-1$. Here, we continue from [1, Eqn. (23)] and re-interpret it as:

$$n\sum_{j=1}^{K} R_j \leq \sum_{j=1,j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_1 \tag{11}$$

$$\leq \underbrace{[h(\mathbf{Y}_i) - nR_i] + \cdots + [h(\mathbf{Y}_i) - nR_i]}_{K-1 \text{ items}} + nc_2 \tag{12}$$

$$= (K-1)h(\mathbf{Y}_i) - (K-1)nR_i + nc_2 \tag{13}$$

$$\leq (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_i + nc_3 \tag{14}$$

where $i \in \{1,\ldots,K\}$ is arbitrary. Here, the second inequality means that we apply [16, 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 (14), dividing both sides by $\frac{n}{2}\log P$, and taking the limit $P \to \infty$ on both sides, we obtain

$$Kd_i + \sum_{j=1,j\neq i}^{K} d_j \leq K-1, \qquad i=1,\ldots,K \tag{15}$$

which is (7) in Theorem 2, completing the converse proof for IC-EE.

V. Converse for K-User IC-CM

When we studied the sum s.d.o.f. of IC-CM, we applied [16, Lemma 2] to [1, Eqn. (44)] by treating the signal from transmitter j as the unintended noise to its neighbor transmitter-receiver pair $j+1$. Here, we continue from [1, Eqn. (44)] and re-interpret it as follows: For any $i \in \{1,\ldots,K\}$, we select

$$k \triangleq \begin{cases} i-1, & \text{if } i \geq 2 \\ K, & \text{if } i = 1 \end{cases} \tag{16}$$

and then have

$$n\sum_{j=1,j\neq i}^{K} R_j \leq \left[\sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j)\right] - h(\mathbf{Y}_i) + nc_4 \tag{17}$$

$$\leq h(\tilde{\mathbf{X}}_k) + \left[\sum_{j=1,j\neq k}^{K} h(\tilde{\mathbf{X}}_j)\right] - h(\mathbf{Y}_i) + nc_5 \tag{18}$$

$$\leq h(\mathbf{Y}_i) - nR_i + \left[\sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) \right] - h(\mathbf{Y}_i) + nc_6 \quad (19)$$

Here, inequality (19) means that we apply [16, Lemma 2] by treating the signal from transmitter k as the unintended noise to the transmitter-receiver pair i. Continuing from (19)

$$n \sum_{j=1, j\neq i}^{K} R_j \leq \left[\sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) \right] - nR_i + nc_6 \quad (20)$$

$$\leq \underbrace{[h(\mathbf{Y}_k) - nR_k] + \cdots + [h(\mathbf{Y}_k) - nR_k]}_{K-1 \text{ items}}$$

$$- nR_i + nc_7 \quad (21)$$

$$= (K-1)h(\mathbf{Y}_k) - (K-1)nR_k - nR_i + nc_7 \quad (22)$$

$$\leq (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_k$$

$$- nR_i + nc_7 \quad (23)$$

which is

$$(K-1)nR_k + n\sum_{j=1}^{K} R_j \leq (K-1)\left(\frac{n}{2}\log P\right) + nc_7 \quad (24)$$

Similarly, inequality (21) means that we apply [16, 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 (24), dividing both sides by $\frac{n}{2}\log P$, and taking the limit $P \to \infty$ on both sides, we obtain

$$Kd_k + \sum_{j=1, j\neq k}^{K} d_j \leq K-1, \qquad k = 1, \ldots, K \quad (25)$$

which is (7) in Theorem 2, completing the converse proof for IC-CM.

VI. Polytope Structure and Extreme Points

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 6 *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:*

$$(0, 0, \ldots, 0), \quad (26)$$

$$\Big(\frac{K-1-p}{K-p}, \underbrace{\frac{1}{K-p}, \ldots, \frac{1}{K-p}}_{p \text{ items}}, \underbrace{0, \ldots, 0}_{m \text{ items}}\Big),$$

$$K-2 \geq p \geq 0, \quad m = K-1-p \geq 1 \quad (27)$$

$$\Big(\underbrace{\frac{1}{2}, \ldots, \frac{1}{2}}_{p' \text{ items}}, \underbrace{0, \ldots, 0}_{m' \text{ items}}\Big),$$

$$K-2 \geq p' \geq 3, \quad m' \geq 1, \quad p' + m' = K \geq 5 \quad (28)$$

$$\Big(\frac{K-1}{2K-1}, \frac{K-1}{2K-1}, \ldots, \frac{K-1}{2K-1}\Big) \quad (29)$$

up to element reordering.

The proof of Theorem 6 is omitted here due to space constraints; see [24] for details. It is worth mentioning that different portions of the region D are governed by different upper bounds. The sum s.d.o.f. tuple, which is symmetric and has no zero elements, is governed by the upper bounds in (7) due to secrecy constraints. However, all other extreme points have zeros as some elements, and therefore are governed by the upper bounds in (8) due to interference constraints in [20], [21]. 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.

Now, in order to show the tightness of region D, it suffices to show the achievability for each structure in Theorem 6. Clearly, the all zero vector in (26) is trivially achievable. The symmetric tuple in (29) is achievable due to [1], [2]. Therefore, it remains to show the achievability of the structures in (27) and (28).

In order to address the achievabilities of (27) and (28), we formulate a new channel model as a $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers. Then, we have the following theorem.

Theorem 7 *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:*

$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}\Big) \quad (30)$$

for almost all channel gains.

The proof of Theorem 7 is also omitted here due to space constraints; see [24] for details. The basic idea is as follows: As shown in (27), 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. The technique we use in the proof of Theorem 7 is asymptotical interference alignment [19] and structured cooperative jamming [10]. The alignment scheme is illustrated in Fig. 2 with $m = 3, p = 2, N = 1$.

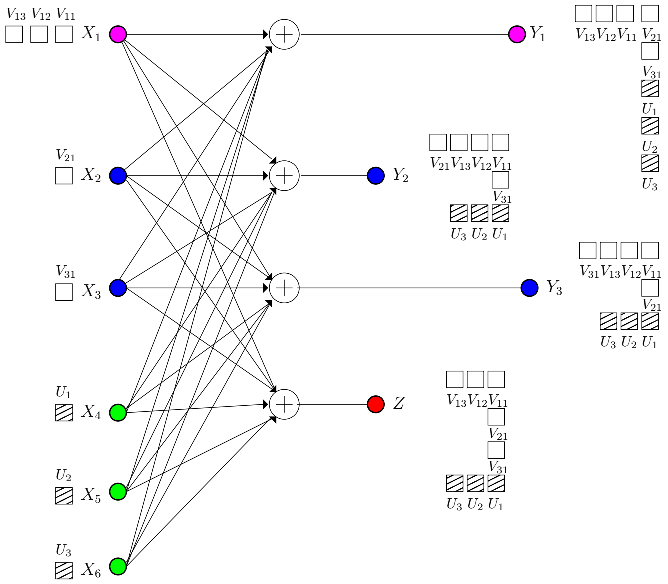

Fig. 2. Illustration of secure interference alignment of Theorem 7 with $m = 3, p = 2, N = 1$.

Here, we provide a few comments about Theorem 7. Theorem 7 provides quite general results, and subsumes some other known cases:

1) The result in [16] is a special case of Theorem 7 with $p = 0, m \geq 1, N = 1$.
2) (27) is a special case of Theorem 7 with $p \geq 0, m = K - 1 - p \geq 1, N = m + 1$.
3) (28) is a byproduct of Theorem 7: 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:

$$\Big(\underbrace{\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}}_{p' \text{ items}}, 0\Big) \tag{31}$$

Now, if we add $m' - 1$ more independent helpers into the network, (28) can be achieved trivially.

Therefore, with the help of Theorem 7, each structure in Theorem 6 can be achieved, which provides the achievability proof for Theorem 2 for $K \geq 3$.

Finally, we address the $K = 2$ case. 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 [1], [2]. The achievabilities of $(\frac{1}{2}, 0), (0, \frac{1}{2})$ are the special cases of Theorem 7 with $p = 0, m = 1, N = 2$.

VII. Conclusions

We determined the *entire s.d.o.f. region* of the K-user IC-EE, K-user IC-CM, and K-user IC-CM-EE. The converse was shown to be dominated by secrecy constraints and interference constraints in different parts. To show the tightness and achieve the region characterized by the converse, we provided a general method to investigate this class of channels, whose s.d.o.f. regions have a polytope structure. We achieved each extreme point by relating it to a specific channel model. More specifically, 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. Then, we achieved the entire polytope converse region by time sharing. Finally, 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.

References

[1] J. Xie and S. Ulukus. Unified secure DoF analysis of K-user Gaussian interference channels. In *IEEE ISIT*, July 2013.

[2] J. Xie and S. Ulukus. Secure degrees of freedom of K-user Gaussian interference channels: A unified view. Submitted to *IEEE Trans. on Information Theory*, May 2013. Also available at [arXiv:1305.7214].

[3] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, October 1949.

[4] A. D. Wyner. The wiretap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, January 1975.

[5] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman. Gaussian wiretap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 1978.

[7] 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*, 54(6):2493–2507, June 2008.

[8] X. He and A. Yener. A new outer bound for the Gaussian interference channel with confidential messages. In *CISS*, March 2009.

[9] O. O. Koyluoglu and H. El Gamal. Cooperative encoding for secrecy in interference channels. *IEEE Trans. Inf. Theory*, 57(9):5681–5694, September 2011.

[10] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, June 2008.

[11] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conference*, September 2008.

[12] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. In *IEEE ITW*, June 2009.

[13] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Trans. Inf. Theory*, 57(6):3323–3332, June 2011.

[14] J. Xie and S. Ulukus. Real interference alignment for the K-user Gaussian interference compound wiretap channel. In *Allerton Conference*, September 2010.

[15] X. He and A. Yener. Providing secrecy with structured codes: Two-user Gaussian channels. *IEEE Trans. Inf. Theory*, 60(4):2121–2138, April 2014.

[16] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *Allerton Conference*, October 2012.

[17] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Trans. Inf. Theory*, 60(6):3359–3378, June 2014.

[18] J. Xie and S. Ulukus. Secure degrees of freedom region of the Gaussian multiple access wiretap channel. In *Asilomar Conference*, November 2013.

[19] 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*, submitted November 2009. Also available at [arXiv:0908.2282].

[20] A. Host-Madsen and A. Nosratinia. The multiplexing gain of wireless networks. In *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[21] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Trans. Inf. Theory*, 54(8):3425–3441, August 2008.

[22] B. Grunbaum. *Convex Polytopes*. Springer, second edition, 2003.

[23] M. Padberg. *Linear Optimization and Extensions*. Springer, second edition, 1999.

[24] J. Xie and S. Ulukus. Secure degrees of freedom regions of multiple access and interference channels: The polytope structure. Submitted to *IEEE Trans. on Information Theory*, April 2014. Also available at [arXiv:1404.7478].