Unified Secure DoF Analysis of K-User Gaussian Interference Channels

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

***Abstract*—We determine the exact sum secure degrees of freedom (d.o.f.) of the K-user Gaussian interference channel. We consider three different secrecy constraints: 1) K-user interference channel with one external eavesdropper (IC-EE), 2) K-user interference channel with confidential messages (IC-CM), and 3) K-user interference channel with confidential messages and one external eavesdropper (IC-CM-EE). We show that for all of these three cases, the exact sum secure d.o.f. is $\frac{K(K-1)}{2K-1}$. We show converses for IC-EE and IC-CM, which imply a converse for IC-CM-EE. We show achievability for IC-CM-EE, which implies achievability for IC-EE and IC-CM. We develop the converses by relating the channel inputs of interfering users to the reliable rates, and by quantifying the secrecy penalty in terms of the eavesdroppers' observations. Our achievability uses structured signalling, channel prefixing via structured cooperative jamming, and asymptotic real interference alignment.**

I. Introduction

In this paper, we study secure communications in multi-user interference networks from an information-theoretic point of view. The security of communication was first studied by Shannon via a noiseless wiretap channel [1]. Noisy wiretap channel was introduced by Wyner who determined its capacity-equivocation region for the degraded case [2]. His result was generalized to arbitrary, not necessarily degraded, wiretap channels by Csiszar and Korner [3], and extended to Gaussian wiretap channels by Leung-Yan-Cheong and Hellman [4]. In recent years, a considerable amount of research work has been devoted to the investigation of information-theoretic security in multi-user networks. In this paper, we focus on K-user interference channels with secrecy constraints.

The K-user Gaussian interference channel with secrecy constraints consists of K transmitter-receiver pairs each wishing to have secure communication over a Gaussian interference channel; see Fig. 1. We consider three different secrecy constraints: 1) K-user interference channel with one external eavesdropper (IC-EE), where K transmitter-receiver pairs wish to have secure communication against an external eavesdropper. 2) K-user interference channel 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 interference channel 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.

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

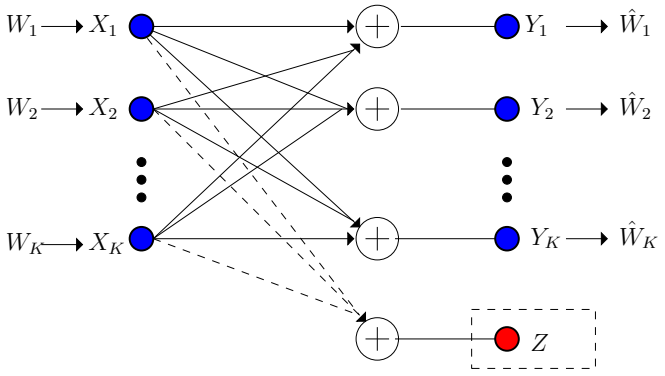

Fig. 1. K-user Gaussian interference wiretap channels.

The two-user IC-CM was studied in [5], [6], and the two-user IC-EE was studied in [7]. The exact secrecy capacity region of either model is unknown, even in the case of Gaussian channels. In the absence of exact secrecy capacity regions, achievable secure degrees of freedom (d.o.f.) at high signal-to-noise ratio (SNR) has been studied, in [8], [9] for IC-CM, and in [9], [10] for IC-EE. Reference [8] showed that nested lattice codes and layered coding are useful in providing positive sum secure d.o.f. for the K-user IC-CM; their result gave a sum secure d.o.f. of less than $\frac{3}{4}$ for $K=3$. Reference [9] used interference alignment to achieve a sum secure d.o.f. of $\frac{K(K-2)}{2K-2}$ for the K-user IC-CM, which gave $\frac{3}{4}$ for $K=3$. Based on the same idea, [9], [10] achieved a sum secure d.o.f. of $\frac{K(K-1)}{2K}$ for the K-user IC-EE, which gave 1 for $K=3$. The approach used in [9], [10] is basically to evaluate the secrecy performance of the interference alignment technique [11] devised originally to determine the sum d.o.f. of the K-user interference channel without any secrecy constraints. Since the original interference alignment scheme puts all of the interfering signals into the same sub-space at a receiver, it naturally provides a certain amount of *secrecy* to those signals as an unintended byproduct, because the interference signals in the same sub-space create uncertainty for one another and make it difficult for the receiver to decode them.

Recently, the *exact* sum secure d.o.f. of the two-user IC-CM was obtained to be $\frac{2}{3}$ in [12]. This reference showed that while interference alignment is a key ingredient in achieving

positive secure d.o.f., a more intricate design of the signals is needed to achieve the simultaneous end-goals of reliability at the desired receivers and secrecy at the eavesdroppers. In particular, in [12], each transmitter sends both message carrying signals, as well as cooperative jamming signals. This random mapping of the message carrying signals to the channel inputs via cooperative jamming signals may be interpreted as channel prefixing [3]. Both the message carrying signals and the cooperative jamming signals come from the same discrete alphabet, and hence are structured. In addition, the signals are carefully aligned at the legitimate receivers and the eavesdroppers using real interference alignment [13].

In this paper, we generalize the results in [12] to the case of K-user interference channel, for $K > 2$. Our generalization has three main components: 1) While [12] considered IC-CM only, we consider both IC-CM and IC-EE and their combination IC-CM-EE in a unified framework. 2) For achievability: In the case of two-user IC-CM, each message needs to be delivered reliably to one receiver and needs to be protected from another receiver. Here, we need to deliver each message to a receiver, while protecting it from K other receivers. This requires designing signals in order to achieve alignment at $K+1$ receivers simultaneously; at one receiver we need alignment to ensure that the largest space is made available to message carrying signals for their reliable decodability, and at K other receivers, we need to align cooperative jamming signals with message carrying signals to protect them. 3) For the converse: To the best of our knowledge, the only known upper bound for the K-user interference channel with secrecy constraints is $\frac{K}{2}$, which is the upper bound with no secrecy constraints [11]. The upper bounding technique in [12] considers a single message each time. Here, we consider all of the messages in the converse of IC-EE and all but one message in the converse of IC-CM, by focusing on the eavesdropper as opposed to the message.

In the following, we show converses seperately for IC-EE and IC-CM, which imply a converse for IC-CM-EE. We show achievability for IC-CM-EE, which implies achievability for IC-EE and IC-CM. The achievability and converse meet giving an exact sum secure d.o.f. of $\frac{K(K-1)}{2K-1}$ for all three models.

II. System Model, Definitions and the Result

The input-output relationships for a K-user Gaussian interference channel with secrecy constraints (Fig. 1) are:

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

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

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 $\{N_1, \ldots, N_K, N_Z\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All the channel gains are time-invariant, and independently drawn from continuous distributions. 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 the message 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. We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_i \triangleq X_i^n$, $\mathbf{Y}_j \triangleq Y_j^n$, $\mathbf{Z} \triangleq Z^n$, etc. The legitimate receiver j decodes the message as $\hat{W}_j$ based on its observation $\mathbf{Y}_j$. A 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, $\max_j \Pr\left[W_j \neq \hat{W}_j\right] \leq \epsilon$, and the corresponding secrecy requirement is satisfied. We consider three different secrecy constraints. In IC-EE, all of the messages are kept information-theoretically secure against the eavesdropper,

$$H(W_1, W_2, \ldots, W_K|\mathbf{Z}) \geq H(W_1, W_2, \ldots, W_K) - n\epsilon \tag{3}$$

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

$$H(W_{-i}^K|\mathbf{Y}_i) \geq H(W_{-i}^K) - n\epsilon, \qquad i = 1, \ldots, K \tag{4}$$

where $W_{-i}^K \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$. Finally, in IC-CM-EE, we impose both secrecy constraints (3) and (4).

The supremum of all sum achievable secrecy rates is the sum secrecy capacity $C_{s,\Sigma}$, and the sum secure d.o.f., $D_{s,\Sigma}$, is defined as

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \frac{C_{s,\Sigma}}{\frac{1}{2}\log P} = \lim_{P\to\infty} \sup \frac{R_1 + \ldots + R_K}{\frac{1}{2}\log P} \tag{5}$$

The main result of this paper is stated in the following theorem.

Theorem 1 *The sum secure d.o.f. of the K-user IC-EE, IC-CM, and IC-CM-EE is $\frac{K(K-1)}{2K-1}$ for almost all channel gains.*

III. Converse for IC-EE

We start with the sum rate:

$$n\sum_{i=1}^{K} R_i = \sum_{i=1}^{K} H(W_i) = H(W_1^K) \tag{6}$$

$$\leq I(W_1^K; \mathbf{Y}_1^K) - I(W_1^K; \mathbf{Z}) + nc_0 \tag{7}$$

$$\leq I(W_1^K; \mathbf{Y}_1^K, \mathbf{Z}) - I(W_1^K; \mathbf{Z}) + nc_0 \tag{8}$$

$$\leq I(\mathbf{X}_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + nc_0 \tag{9}$$

$$= h(\mathbf{Y}_1^K|\mathbf{Z}) - h(\mathbf{N}_1^K|\mathbf{Z}, \mathbf{X}_1^K) + nc_0 \tag{10}$$

$$\leq h(\mathbf{Y}_1^K|\mathbf{Z}) + nc_1 \tag{11}$$

$$= h(\mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_1 \tag{12}$$

where $W_1^K \triangleq \{W_j\}_{j=1}^K$, $\mathbf{X}_1^K \triangleq \{\mathbf{X}_j\}_{j=1}^K$, $\mathbf{Y}_1^K \triangleq \{\mathbf{Y}_j\}_{j=1}^K$, and all the c_is in this paper are constants which do not depend on P. For each j, let us introduce $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, where $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$ which is zero-mean Gaussian with variance $\sigma_j^2 < \min(\min_i 1/h_{ji}^2, 1/g_j^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables. Continuing from (12),

$$\begin{aligned} n\sum_{i=1}^K R_i &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{Z}) \\ &\quad - h(\mathbf{Z}) + nc_1 && (13)\\ &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{X}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) \\ &\quad - h(\mathbf{Z}) + nc_1 && (14)\\ &= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{N}}_1^K) - h(\mathbf{Z}) + nc_1 && (15)\\ &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_2 && (16)\\ &= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_2 && (17)\\ &\le h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_3 && (18)\end{aligned}$$

where $\tilde{\mathbf{X}}_1^K \triangleq \{\tilde{\mathbf{X}}_j\}_{j=1}^K$, and the last inequality is due to the fact that, $h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) \le nc'$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be *reconstructed*. A similar proof can be found in [14, Eqn. (30)-(34)].

Next, we note

$$h(\tilde{\mathbf{X}}_j) \le h(g_j\mathbf{X}_j + \mathbf{N}_Z) + nc_4 \le h(\mathbf{Z}) + nc_4 \quad (19)$$

where the inequalities are due to the differential entropy version of [15, Problem 2.14]. Inserting (19) into (18), for any $j = 1, \ldots, K$, we get

$$\begin{aligned} n\sum_{i=1}^K R_i &\le \sum_{i=1}^K h(\tilde{\mathbf{X}}_i) - h(\mathbf{Z}) + nc_3 && (20)\\ &\le \sum_{i=1, i\ne j}^K h(\tilde{\mathbf{X}}_i) + nc_5 && (21)\end{aligned}$$

which means that the net effect of the presence of an eavesdropper is to *eliminate* one of the channel inputs; we call this the *secrecy penalty*.

Next, we recall Lemma 2 in [14], which states that, for reliable decoding of message k at receiver k, any (slightly noisy version of) channel input from transmitter $i, i \ne k$, must satisfy:

$$h(\tilde{\mathbf{X}}_i) \le h(\mathbf{Y}_k) - nR_k + nc \quad (22)$$

We apply (22) to each $\tilde{\mathbf{X}}_i$ with $k = i-1$ (for $i = 1$, $k = K$),

$$\begin{aligned} n\sum_{i=1}^K R_i &\le \sum_{i=1, i\ne j}^K h(\tilde{\mathbf{X}}_i) + nc_5 && (23)\\ &\le [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + \cdots \\ &\quad + [h(\mathbf{Y}_{j-2}) - nR_{j-2}] + [h(\mathbf{Y}_j) - nR_j] \\ &\quad + \cdots + [h(\mathbf{Y}_{K-1}) - nR_{K-1}] + nc_6 && (24)\end{aligned}$$

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

$$2n\sum_{i=1}^K R_i \le (K-1)\frac{n}{2}\log P + nR_j + nc_7 \quad (25)$$

Therefore, we have a total of K bounds in (25) for $j = 1, \ldots, K$. Summing these K bounds, we obtain:

$$(2K-1)n\sum_{i=1}^K R_i \le K(K-1)\frac{n}{2}\log P + nc_8 \quad (26)$$

which gives

$$D_{s,\Sigma} \le \frac{K(K-1)}{2K-1} \quad (27)$$

completing the converse for IC-EE.

IV. Converse for IC-CM

We focus on the secrecy constraint (4) at a single receiver, say j, as an eavesdropper, and start with the sum rate corresponding to all unintended messages:

$$\begin{aligned} n\sum_{i=1, i\ne j}^K R_i &= \sum_{i=1, i\ne j}^K H(W_i) = H(W_{-j}^K) && (28)\\ &\le I(W_{-j}^K; \mathbf{Y}_{-j}^K) - I(W_{-j}^K; \mathbf{Y}_j) + nc_9 && (29)\\ &\le I(W_{-j}^K; \mathbf{Y}_{-j}^K, \mathbf{Y}_j) - I(W_{-j}^K; \mathbf{Y}_j) + nc_9 && (30)\\ &\le I(\mathbf{X}_{-j}^K; \mathbf{Y}_{-j}^K|\mathbf{Y}_j) + nc_9 && (31)\\ &= h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_{-j}^K) + nc_9 && (32)\\ &\le h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_1^K) + nc_9 && (33)\\ &= h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{N}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_1^K) + nc_9 && (34)\\ &\le h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) + nc_{10} && (35)\\ &= h(\mathbf{Y}_{-j}^K, \mathbf{Y}_j) - h(\mathbf{Y}_j) + nc_{10} && (36)\\ &= h(\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{10} && (37)\end{aligned}$$

where $\mathbf{X}_{-j}^K \triangleq \{\mathbf{X}_i\}_{i=1, i\ne j}^K$, $\mathbf{Y}_{-j}^K \triangleq \{\mathbf{Y}_i\}_{i=1, i\ne j}^K$, and $\mathbf{N}_{-j}^K \triangleq \{\mathbf{N}_i\}_{i=1, i\ne j}^K$. For each j, let us introduce $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, where $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$ which is zero-mean Gaussian with variance $\sigma_j^2 < \min_i 1/h_{ji}^2$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables. Continuing from (37),

$$\begin{aligned} &n\sum_{i=1, i\ne j}^K R_i \\ &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{10} && (38)\\ &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{X}_1^K) \\ &\quad - h(\mathbf{Y}_j) + nc_{10} && (39)\\ &= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{N}}_1^K|\mathbf{Y}_1^K, \mathbf{X}_1^K) \\ &\quad - h(\mathbf{Y}_j) + nc_{10} && (40)\\ &\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{11} && (41)\\ &= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{11} && (42)\\ &\le h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{12} && (43)\end{aligned}$$

where the last inequality is due to the fact that, $h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) \leq nc''$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be *reconstructed*.

Next, we apply Lemma 2 in [14] shown in (22) to each $\tilde{\mathbf{X}}_i$ with $k = i+1$ (for $i = K$, $k = 1$),

$$n \sum_{i=1, i\neq j}^{K} R_i \leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_j) + nc_{12} \tag{44}$$

$$\leq \sum_{i=1}^{K} [h(\mathbf{Y}_i) - nR_i] - h(\mathbf{Y}_j) + nc_{13} \tag{45}$$

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

$$nR_j + 2n \sum_{i=1, i\neq j}^{K} R_i \leq \sum_{i=1, i\neq j}^{K} h(\mathbf{Y}_i) + nc_{13} \tag{46}$$

$$\leq (K-1)\frac{n}{2}\log P + nc_{14} \tag{47}$$

Therefore, we have a total of K bounds in (47) for $j = 1, \ldots, K$. Summing these K bounds, we obtain:

$$(2K-1)n \sum_{i=1}^{K} R_i \leq K(K-1)\frac{n}{2}\log P + nc_{15} \tag{48}$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{49}$$

completing the converse for IC-CM.

V. Achievability

We provide achievability for the K-user IC-CM-EE, which will imply achievability for K-user IC-EE and IC-CM. We first summarize the achievability scheme in [12] devised for the two-user IC-CM. In [12], four mutually independent discrete random variables $\{V_1, U_1, V_2, U_2\}$ are employed. Each of them is uniformly and independently drawn from the same discrete constellation $C(a, Q)$

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{50}$$

The role of V_i is to carry message W_i, and the role of U_i is to cooperatively jam receiver i to help transmitter-receiver pair j, where $j \neq i$, for $i, j = 1, 2$. By carefully selecting the transmit coefficients, U_1 and V_2 are aligned in the same *dimension* at receiver 1, and U_2 and V_1 are aligned in the same *dimension* at receiver 2; and therefore, U_1 protects V_2, and U_2 protects V_1. By this signalling scheme, information leakage rates are upper bounded by constants, and the message rates are made to scale with power P, reaching the secure d.o.f. capacity of the two-user IC-CM which is $\frac{2}{3}$.

Here, for the K-user IC-CM-EE, we employ a total of K^2 random variables,

$$V_{ij}, \quad i, j = 1, \ldots, K,\ j \neq i \tag{51}$$

$$U_k, \quad k = 1, \ldots, K \tag{52}$$

which are illustrated in Fig. 2. The scheme proposed here has

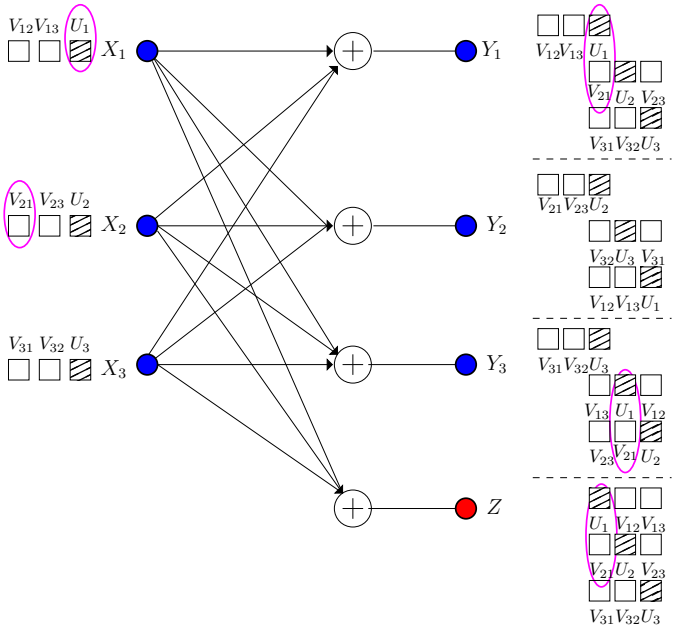

Fig. 2. Illustration of alignment for 3-user IC-CM-EE. U_1 and V_{21} are marked to emphasize their simultaneous alignment at Y_1, Y_3 and Z.

two major differences from [12]: 1) Instead of using a single random variable to carry a message, we use a total of $K-1$ random variables to carry each message. For transmitter i, $K-1$ random variables $\{V_{ij}\}_{j\neq i}$, each representing a sub-message, collectively carry message W_i. 2) Rather than protecting one message at one receiver, each U_k simultaneously protects a portion of all sub-messages at all required receivers. More specifically, U_k protects $\{V_{ik}\}_{i\neq k,j}$ at receivers j, and at the eavesdropper (if there is any). For example, in Fig 2, U_1 protects V_{21} and V_{31} where necessary. In particular, U_1 protects V_{21} at receivers 1, 3 and the eavesdropper; and it protects V_{31} at receivers 1, 2 and the eavesdropper. As a technical challenge, this requires U_1 to be aligned with the same signal, say V_{21}, at multiple receivers simultaneously, i.e., at receivers 1, 3 and the eavesdropper. These alignments are circled by ellipsoids in Fig 2. We do these simultaneous alignments using asymptotic real alignment technique proposed in [16] and used in [10], [17].

For illustration purposes, we demonstrate how we can align U_1 with V_{21} at Y_1 and Y_3, simultaneously. Towards this end, instead of using one random variable V_{21} for each sub-message, we employ a large number of random variables denoted as $V_{21} \triangleq \{v_{21t} : t = 1, \ldots, |T_1|\}$ each corresponding to one element of the following set serving as *dimensions*:

$$T_1 = \alpha_1\{h_{11}^{r_{11}} h_{21}^{r_{21}} h_{13}^{r_{13}} h_{23}^{r_{23}} : r_{11}, r_{21}, r_{13}, r_{23} \in \{0, \ldots, m\}\} \tag{53}$$

where m is a large constant, which will be specified later, and α_1 is a constant independently drawn from the same continuous distribution as channel gains to separate U_1 from other $\{U_i\}_{i\neq 1}$. To perform the alignment, U_1 has the same detailed structure as V_{21}, i.e., $U_1 \triangleq \{u_{1t} : t = 1, \ldots, |T_1|\}$.

At receiver 1, the elements of U_1 from transmitter 1 occupy the dimensions $h_{11}T_1$ and the elements of V_{21} from transmitter 2 occupy the dimensions $h_{21}T_1$. Although these two sets are not the same, their intersection contains nearly as many elements as T_1, i.e.,

$$|h_{11}T_1 \cap h_{21}T_1| = (m+1)^2 m^2 \approx (m+1)^4 = |T_1| \quad (54)$$

when m is large, i.e., almost all elements of U_1 and V_{21} are asymptotically aligned at receiver 1. The same argument applies to the alignment at receiver 3; this is shown in Fig. 3. Therefore, the overall alignment described in Fig. 2 can be implemented by designing the *dimension* sets in $\{T_i\}_{i=1}^K$ more intricately. Finally, the following theorem is used to evaluate achievable secrecy rates with this alignment scheme.

Theorem 2 *For the K-user IC-CM-EE, the following rate tuple is achievable*

$$R_i \geq I(V_i;Y_i) - \max_{j\in\{0,1,\ldots,K\}\setminus\{i\}} I(V_i;Y_j|V_{-i}) \quad (55)$$

where $i \in \{1,\ldots,K\}$ and for convenience we denote Z by Y_0. The auxiliary random variables $\{V_i\}_{i=1}^K$ are mutually independent, and for each i, we have the following Markov chain $V_i \to X_i \to (Y_1,\ldots,Y_K)$.

This theorem can be proved by focusing on each transmitter and considering the associated compound wiretap channel with enhanced eavesdroppers.

We then apply our alignment scheme in (55) by selecting

$$V_i \triangleq \{V_{ij}\}_{j\neq i} = \left\{\{v_{ijt_j} : t_j = 1,\ldots,|T_j|\} : j \neq i\right\} \quad (56)$$

for $i = 1,\ldots,K$. For any $\delta > 0$, by using the Khintchine-Groshev theorem of Diophantine approximation in number theory and selecting a, Q in (50) appropriately according to δ and P, the probability of error in detecting V_i as $\hat{V}_i$ based on Y_i can be upper bounded by a function decreasing exponentially fast with P. Then, by Fano's inequality, we have $H(V_i|Y_i) \leq o_P$ where o_P is a function that is $o(\log P)$, and

$$I(V_i;Y_i) \geq \frac{K-1}{K-1+K\left(\frac{m+2}{m+1}\right)^{K^2+1}+\delta} \cdot \frac{1}{2}\log P + o_P \quad (57)$$

which provides a lower bound for the first term in (55).

On the other hand, due to the property in (54) of asymptotic alignment, we can upper bound the second term in (55) as

$$I(V_i;Y_j|V_{-i}) \leq \frac{K\left(\frac{2m+1}{m^2+2m+1}\right)}{K-1+K\left(\frac{m+2}{m+1}\right)^{K^2+1}+\delta} \cdot \frac{1}{2}\log P + o_P \quad (58)$$

for $j = 0,1,\ldots,K$ and $j \neq i$.

Combining (57) and (58), (55) can be lower bounded as

$$R_i \geq \frac{(K-1)-K\left(\frac{2m+1}{m^2+2m+1}\right)}{K-1+K\left(\frac{m+2}{m+1}\right)^{K^2+1}+\delta} \cdot \frac{1}{2}\log P + o_P \quad (59)$$

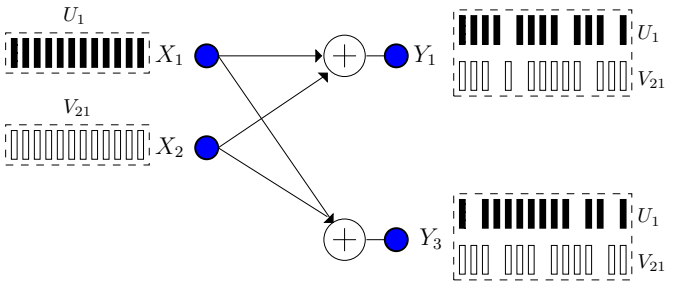

Fig. 3. Illustration of simultaneous alignment at multiple receivers.

By choosing $m \to \infty$ and $\delta \to 0$, each individual secrecy rate R_i can arbitrarily approach $\frac{K-1}{2K-1} \cdot \frac{1}{2}\log P$, thereby giving a lower bound for the sum secure d.o.f. as

$$D_{s,\Sigma} \geq \frac{K(K-1)}{2K-1} \quad (60)$$

The achievability in (60) and the converses in (27) and (49) give the exact sum secure d.o.f. of the K-user IC-CM-EE as

$$D_{s,\Sigma} = \frac{K(K-1)}{2K-1} \quad (61)$$

REFERENCES

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

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

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

[4] S. K. Leung-Yan-Cheong and M. E. Hellman. Gaussian wiretap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 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*, 54(6):2493–2507, June 2008.

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

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

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

[9] 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.

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

[11] 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.

[12] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Trans. on Inf. Theory*, submitted September 2012. Also available at [arXiv:1209.5370].

[13] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Trans. Inf. Theory*, submitted August 2009. Also available at [arXiv:0908.1208].

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

[15] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, second edition, 2006.

[16] 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].

[17] A. Khisti. Interference alignment for the multiantenna compound wiretap channel. *IEEE Trans. Inf. Theory*, 57(5):2976–2993, May 2011.