Secure Degrees of Freedom of K-User Gaussian Interference Channels: A Unified View

Jianwei Xie and Sennur Ulukus, *Member, IEEE*

***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 $K(K-1)/(2K-1)$. 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. Our converse is based on developing a direct relationship between the differential entropies of the channel inputs and the rates of the users, and quantifying the effect of eavesdropping on the rates in terms of the differential entropies of the eavesdroppers' observations. Our achievability is based on structured signaling, structured cooperative jamming, channel prefixing, and asymptotic real interference alignment. While the traditional interference alignment provides some amount of secrecy by mixing unintended signals in a smaller subspace at every receiver, in order to attain the optimum sum secure d.o.f., we incorporate structured cooperative jamming into the achievable scheme, and intricately design the structure of all of the transmitted signals jointly.**

***Index Terms*— Wiretap channel, interference channel, secure degrees of freedom, cooperative jamming, 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]. This line of research has been subsequently extended to many multi-user settings, e.g., broadcast channels with confidential messages [5], [6], multi-receiver wiretap channels [7]–[10] (see also a survey on extensions of these to MIMO channels [11]), interference channels with confidential messages [5], [12], interference channels with external eavesdroppers [13], multiple access wiretap channels [14]–[18], wiretap channels with helpers [19], relay eavesdropper channels [20]–[25], compound wiretap channels [26], [27], etc. While the channel models involving a single transmitter, such as broadcast channels with confidential messages and multi-receiver wiretap channels, are relatively better understood, the channel models involving multiple independent transmitters, such as interference channels with confidential messages and/or external eavesdroppers, multiple access wiretap channels, wiretap channels with helpers, and relay-eavesdropper channels, are much less understood. The exact secrecy capacity regions of all these multiple-transmitter models remain unknown, even in the case of simple 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) regimes has been studied in the literature [28]–[41]. In this paper, we focus on the K-user interference channel with secrecy constraints, and determine its exact sum secure d.o.f.

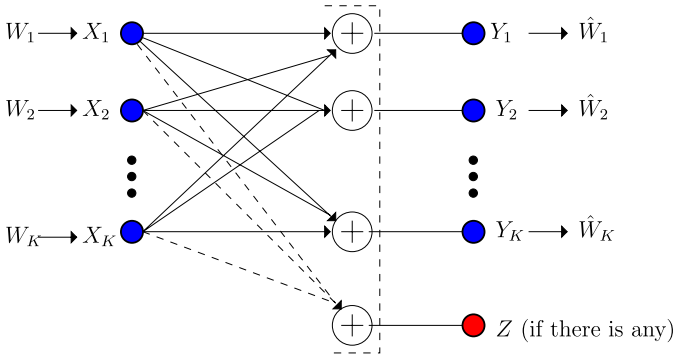

Fig. 1. K-user Gaussian interference channel with secrecy constraints.

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 (IC); 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

Manuscript received May 27, 2013; revised June 20, 2014; accepted February 25, 2015. Date of publication March 9, 2015; date of current version April 17, 2015. This work was supported by NSF 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 International Symposium on Information Theory.

J. Xie was with the Department of Electrical and Computer Engineering, University of Maryland at College Park, 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 at College Park, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Communicated by A. B. Wagner, 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.2015.2411260

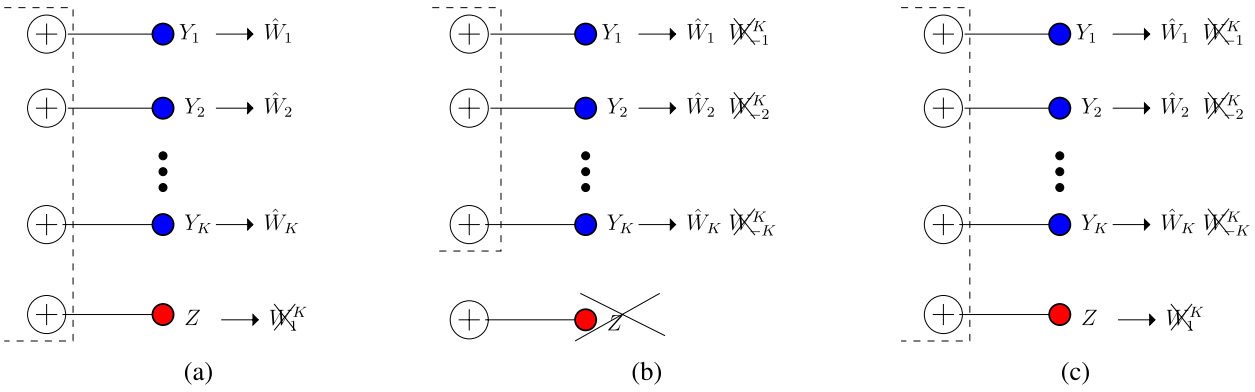

Fig. 2. The receiver sides of the three channel models: (a) K-user IC-EE, (b) K-user IC-CM, and (c) K-user IC-CM-EE, where $W_{-i}^{K} \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

eavesdropper, see Fig. 2(a). 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, see Fig. 2(b). 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 remaining $K-1$ receivers and the external eavesdropper, see Fig. 2(c).

In the Gaussian wiretap channel, the secrecy capacity is the difference between the channel capacities of the transmitter-receiver and the transmitter-eavesdropper pairs [4]. It is well-known that this difference does not scale with the SNR, and hence the secure d.o.f. of the Gaussian wiretap channel is zero, indicating a severe penalty due to secrecy in this case. Fortunately, this does not hold in most multi-user scenarios, including the interference channel. Reference [28] 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 [29] 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, [29], [30] 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 [29] and [30] is basically to evaluate the secrecy performance of the interference alignment technique [42] devised originally for the K-user interference channel without any secrecy constraints. Since the original interference alignment scheme puts all of the interfering signals into the same reduced-dimensionality 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 this sub-space create uncertainty for one another and make it difficult for the receiver to decode them. However, since the end-goal of [42] is *only* to achieve reliable decoding of the transmitted messages at their intended receivers, the d.o.f. it provides is sub-optimal when *both* secrecy and reliability of messages are considered.

Recently, the *exact* sum secure d.o.f. of the two-user IC-CM was obtained to be $\frac{2}{3}$ in [38]. 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 [38], 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 [43]. In particular, at each receiver, the unintended message and both jamming signals are constrained in the same interference sub-space, providing an interference-free sub-space for the intended message. Further, inside the interference sub-space, each unintended message is protected by aligning it with the jamming signal from the other transmitter. Such a perfect alignment provides a constant upper bound for the information leakage rate.

In this paper, we generalize the results in [38] to the case of K-user interference channel, for $K > 2$. Our generalization has three main components:

1) While [38] considered IC-CM only, we consider both IC-CM and IC-EE and their combination IC-CM-EE in a unified framework. To this end, we show converses separately for IC-EE and IC-CM, which imply a converse for IC-CM-EE; and 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.
2) For achievability: In the case of two-user IC-CM in [38], each message needs to be delivered reliably to one receiver and needs to be protected from another receiver. This requires alignment at two receivers, which is achieved in [38] by simply choosing transmission coefficients properly, which cannot be extended to the K-user case here. In the K-user IC-CM-EE case, 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 (desired 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. These requirements create two challenges: i) aligning multiple signals simultaneously at multiple receivers, and ii) upper bounding the information leakage rates by suitable functions which can be made small. We overcome these challenges by using an asymptotical approach [44], where we introduce many signals that carry each message and align them simultaneously at multiple receivers only order-wise (i.e., align most of them, but not all of them), and by developing a method to upper bound the information leakage rate by a function which can be made small. In contrast to the constant upper bound for the information leakage rate in [38], here the upper bound is not constant, but a function which can be made small. This is due to the non-perfect (i.e., only asymptotical) alignment.

3) For the converse: To the best of our knowledge, the only known upper bound for the sum secure d.o.f. of the K-user interference channel with secrecy constraints is $\frac{K}{2}$, which is the upper bound with no secrecy constraints [42]. The upper bounding technique for the two-user IC-CM in [38] considers one single confidential message against the corresponding unintended receiver each time, since in that case the eavesdropping relationship is straightforward: for each message there is only one eavesdropper and for each eavesdropper there is only one confidential message. However, in the case of K-user IC, each message is required to be kept secret against multiple eavesdroppers and each eavesdropper is associated with multiple unintended messages. To develop a tight converse, we focus on the eavesdropper as opposed to the message. In the converse for IC-EE, we consider the sum rate of all of the messages eavesdropped by the external eavesdropper. We sequentially apply the *role of a helper lemma* in [38] to each transmitter by treating its signal as a helper to another specific transmitter. In the converse for IC-CM, for each receiver (which also is an eavesdropper), we consider the sum rate of all unintended messages, and again apply the *role of a helper lemma* in a specific structure.

II. System Model, Definitions and the Result

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

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

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

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 independently drawn from continuous distributions.[1] Once they are generated, the channel gains are fixed (time-invariant) throughput the communication session and are known to all entities. 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 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, Fig. 2(a), all of the messages are kept information-theoretically secure against the external eavesdropper,
$$H(W_1, \ldots, W_K|\mathbf{Z}) \geq H(W_1, \ldots, W_K) - n\epsilon \tag{4}$$
2) In IC-CM, Fig. 2(b), all unintended messages are kept information-theoretically secure against each receiver,
$$H(W_{-i}^K|\mathbf{Y}_i) \geq H(W_{-i}^K) - n\epsilon, \quad i = 1, \ldots, K \tag{5}$$
where $W_{-i}^K \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.
3) In IC-CM-EE, Fig. 2(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 (4) and (5).

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

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \frac{C_{s,\Sigma}}{\frac{1}{2}\log P} = \lim_{P\to\infty} \sup \frac{R_1 + \cdots + R_K}{\frac{1}{2}\log P} \tag{6}$$

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.

[1]For a discussion about complex channel gains, please see [38, Sec. X-C].

We now remark on the *for almost all channel gains* statement in Theorem 1. Our converse proof is valid for all fixed channel gains. On the other hand, our achievability is valid for almost all channel gains. Similar to the discussion in [38, Sec. X.B], there exists a set of channel gains $\mathcal{A}$ in the space of all channel gains, where our achievability proof is not valid. Such an example set of channel gains is obtained when all of the channel gains are the same, e.g.,

$$h_{ji} = g_j = 1 \quad \forall i, j \tag{7}$$

In this case, we have zero sum secure d.o.f. since all the receivers have statistically identical observations. More generally, the achievability proof does not work for rational channel gains. This is typical of achievability schemes that use real interference alignment, see for instance [36], [44]–[46]. Fortunately, such a set $\mathcal{A}$ has zero Lebesgue measure, and this is what we mean by *for almost all channel gains*.[2]

III. Preliminaries

A. Role of a Helper Lemma

For completeness, we repeat [38, Lemma 2] here, which is called *role of a helper lemma*. This lemma identifies a constraint on the signal of a given transmitter, based on the decodability of another transmitter's message at its intended receiver.

Lemma 1 ([38]): For reliable decoding of the kth transmitter's signal at the kth receiver, the channel input of transmitter $i \neq k$, $\mathbf{X}_i$, must satisfy

$$h(\mathbf{X}_i + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_k) - nR_k + nc \tag{8}$$

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

Lemma 1 gives an upper bound on the differential entropy of (a noisy version of) the signal of any given transmitter, transmitter i in (8), in terms of the differential entropy of the channel output and the message rate $nR_k = H(W_k)$, of a user k, based on the decodability of message W_k at its intended receiver. The inequality in this lemma, (8), can alternatively be interpreted as an upper bound on the message rate, i.e., on nR_k, in terms of the difference of the differential entropies of the channel output of a receiver k and the channel input of a transmitter i; in particular, the higher the differential entropy of the signal coming from user i, the lower this upper bound will be on the rate of user k. This motivates not using i.i.d. Gaussian signals which have the highest differential entropy. Also note that this lemma does not involve any secrecy constraints, and is based only on the decodability of the messages at their intended receivers.

[2]This will be reflected by qualifier *for almost all channel gains* in equations (107), (121), and (129) during the achievability proof, i.e., these equations are only correct if the channel gains are not in the set $\mathcal{A}$, i.e., they are correct *for almost all channel gains*.

B. Real Interference Alignment

In this subsection, we review pulse amplitude modulation (PAM) and real interference alignment [43], [44], similar to the review in [36, Sec. III] and [38, Sec. III.C]. 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 Section VI.

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

$$Y = X + N \tag{9}$$

with additive Gaussian noise N 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,

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{10}$$

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

$$\Pr(e) = \Pr\left[X \neq \hat{X}\right] \leq \exp\left(-\frac{d^2_{min}}{8\sigma^2}\right) = \exp\left(-\frac{a^2}{8\sigma^2}\right) \tag{11}$$

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

$$R = \log(2Q+1) \tag{12}$$

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

$$\Pr(e) \leq \exp\left(-\frac{\gamma^2 P^{\delta}}{8\sigma^2}\right) \text{ and } R \geq \frac{1-\delta}{2}\log P \tag{13}$$

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 [44] and [46], 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:

$$\begin{aligned} R' &= I(X;Y) && (14)\\ &\geq I(X;\hat{X}) && (15)\\ &= H(X) - H(X|\hat{X}) && (16)\\ &= \log(2Q+1) - H(X|\hat{X}) && (17)\\ &\geq \log(2Q+1) - 1 - \Pr(e)\log(2Q+1) && (18)\\ &\geq \left[1 - \Pr(e)\right]\frac{1-\delta}{2}\log P - 1 && (19) \end{aligned}$$

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 (19) with arbitrary reliability, where for any fixed P, $\Pr(e)$ in (19) is the probability of error of the PAM scheme given in (13), which is a well-defined function of P. For a finite P, while $\Pr(e)$ may not be arbitrarily small, the rate achieved in (19), which is smaller than the rate of PAM in (12), is achieved arbitrarily reliably. We finally note that as P goes to infinity $\Pr(e)$ goes to zero exponentially, and from (19), both PAM transmission rate and the Shannon achievable rate have the same asymptotical performance, i.e., PAM transmission rate has 1 Shannon d.o.f.

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

$$x = \mathbf{c}^T \mathbf{b} = \sum_{i=1}^{L} c_i b_i \tag{20}$$

where $c_1, \ldots, c_L$ are rationally independent real numbers,[3] and each b_i is drawn independently from the constellation $C(a, Q)$ in (10). 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, [43], [44] 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

$$d_{min} \geq \frac{k_\delta a}{Q^{L-1+\delta}} \tag{21}$$

for almost all rationally independent $\{c_i\}_{i=1}^L$, 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 [36, Proposition 3].

Lemma 2 ([43], [44]): For any small enough $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose

$$Q = P^{\frac{1-\delta}{2(L+\delta)}} \quad \text{and} \quad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{22}$$

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

$$\Pr(e) \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{23}$$

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

Furthermore, as a simple extension, if b_i are drawn independently from different constellations $C_i(a, Q_i)$, the lower bound in (21) can be modified as

$$d_{min} \geq \frac{k_\delta a}{(\max_i Q_i)^{L-1+\delta}} \tag{24}$$

[3] $c_1, \ldots, c_L$ are rationally independent if whenever $q_1, \ldots, q_L$ are rational numbers then $\sum_{i=1}^L q_i c_i = 0$ implies $q_i = 0$ for all i.

IV. Converse for IC-EE

In this section, we develop a converse for the K-user IC-EE (see Fig. 2(a)) defined in (1) and (2) with the secrecy constraint (4). We start with the sum rate:

$$\begin{aligned}
n\sum_{i=1}^{K} R_i &= \sum_{i=1}^{K} H(W_i) = H(W_1^K) && (25)\\
&\leq I(W_1^K; \mathbf{Y}_1^K) - I(W_1^K; \mathbf{Z}) + nc_0 && (26)\\
&\leq I(W_1^K; \mathbf{Y}_1^K, \mathbf{Z}) - I(W_1^K; \mathbf{Z}) + nc_0 && (27)\\
&= I(W_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + nc_0 && (28)\\
&\leq I(\mathbf{X}_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + nc_0 && (29)\\
&= h(\mathbf{Y}_1^K|\mathbf{Z}) - h(\mathbf{Y}_1^K|\mathbf{Z}, \mathbf{X}_1^K) + nc_0 && (30)\\
&= h(\mathbf{Y}_1^K|\mathbf{Z}) - h(\mathbf{N}_1^K|\mathbf{Z}, \mathbf{X}_1^K) + nc_0 && (31)\\
&\leq h(\mathbf{Y}_1^K|\mathbf{Z}) + nc_1 && (32)\\
&= h(\mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_1 && (33)
\end{aligned}$$

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 Sections IV and V are constants which do not depend on P.

For each j, we 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 a zero-mean Gaussian random variable 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 (33),

$$\begin{aligned}
n\sum_{i=1}^{K} R_i &\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_1 && (34)\\
&\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{X}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_1 && (35)\\
&= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{N}}_1^K) - h(\mathbf{Z}) + nc_1 && (36)\\
&\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_2 && (37)\\
&= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_2 && (38)\\
&\leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_3 && (39)
\end{aligned}$$

where $\tilde{\mathbf{X}}_1^K \triangleq \{\tilde{\mathbf{X}}_j\}_{j=1}^K$, and the last inequality is due to the fact that $h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) \leq nc'$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be *reconstructed*, which is shown as follows

$$\begin{aligned}
h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) &\leq \left[\sum_{j=1}^{K} h(\mathbf{Y}_j|\tilde{\mathbf{X}}_1^K)\right] + h(\mathbf{Z}|\tilde{\mathbf{X}}_1^K) && (40)\\
&= \left[\sum_{j=1}^{K} h\left(\sum_{i=1}^{K} h_{ij}(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right)\right]\\
&\quad + h\left(\sum_{i=1}^{K} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_Z \middle| \tilde{\mathbf{X}}_1^K\right) && (41)\\
&= \left[\sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right)\right]\\
&\quad + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_Z \middle| \tilde{\mathbf{X}}_1^K\right) && (42)
\end{aligned}$$

$$\leq \left[\sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j\right)\right] + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_Z\right) \quad (43)$$

$$\stackrel{\triangle}{=} nc_4 \quad (44)$$

Next, we note, for $j = 1, \ldots, K$,

$$h(\tilde{\mathbf{X}}_j) \leq h(g_j\mathbf{X}_j + \mathbf{N}_Z) + nc_5 \leq h(\mathbf{Z}) + nc_5 \quad (45)$$

where the inequalities are due to the differential entropy version of [47, Problem 2.14]. Inserting (45) into (39), for any $j = 1, \ldots, K$, we get

$$n\sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_3 \quad (46)$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Z}) + nc_3 \quad (47)$$

$$\leq \sum_{i=1,i\neq j}^{K} h(\tilde{\mathbf{X}}_i) + nc_6 \quad (48)$$

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*.

We apply the *role of a helper lemma*, Lemma 1, to each $\tilde{\mathbf{X}}_i$ with $k = i + 1$ (for $i = K$, $k = 1$), in (48) as

$$n\sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + \cdots + h(\tilde{\mathbf{X}}_{j-1}) + h(\tilde{\mathbf{X}}_{j+1}) + \cdots + h(\tilde{\mathbf{X}}_K) + nc_7 \quad (49)$$

$$\leq [h(\mathbf{Y}_2) - nR_2] + [h(\mathbf{Y}_3) - nR_3] + \cdots + \left[h(\mathbf{Y}_j) - nR_j\right] + \left[h(\mathbf{Y}_{j+2}) - nR_{j+2}\right] + \cdots + [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + nc_8 \quad (50)$$

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

$$2n\sum_{i=1}^{K} R_i \leq (K-1)\left(\frac{n}{2}\log P\right) + nR_{(j+1) \bmod K} + nc_9 \quad (51)$$

for $j = 1, \ldots, K$. Therefore, we have a total of K bounds in (51) for $j = 1, \ldots, K$. Summing these K bounds, we obtain:

$$(2K-1)n\sum_{i=1}^{K} R_i \leq K(K-1)\left(\frac{n}{2}\log P\right) + nc_{10} \quad (52)$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \quad (53)$$

completing the converse for IC-EE.

V. Converse for IC-CM

In this section, we develop a converse for the K-user IC-CM (see Fig. 2(b)). We focus on the secrecy constraint (5) at a single receiver, say j, as an eavesdropper, and start with the sum rate corresponding to all unintended messages at receiver j:

$$n\sum_{i=1,i\neq j}^{K} R_i = \sum_{i=1,i\neq j}^{K} H(W_i) = H(W_{-j}^K) \quad (54)$$

$$\leq I(W_{-j}^K; \mathbf{Y}_{-j}^K) - I(W_{-j}^K; \mathbf{Y}_j) + nc_{11} \quad (55)$$

$$\leq I(W_{-j}^K; \mathbf{Y}_{-j}^K, \mathbf{Y}_j) - I(W_{-j}^K; \mathbf{Y}_j) + nc_{11} \quad (56)$$

$$= I(W_{-j}^K; \mathbf{Y}_{-j}^K|\mathbf{Y}_j) + nc_{11} \quad (57)$$

$$\leq I(\mathbf{X}_{-j}^K; \mathbf{Y}_{-j}^K|\mathbf{Y}_j) + nc_{11} \quad (58)$$

$$= h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_{-j}^K) + nc_{11} \quad (59)$$

$$\leq h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_1^K) + nc_{11} \quad (60)$$

$$= h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) - h(\mathbf{N}_{-j}^K|\mathbf{Y}_j, \mathbf{X}_1^K) + nc_{11} \quad (61)$$

$$\leq h(\mathbf{Y}_{-j}^K|\mathbf{Y}_j) + nc_{12} \quad (62)$$

$$= h(\mathbf{Y}_{-j}^K, \mathbf{Y}_j) - h(\mathbf{Y}_j) + nc_{12} \quad (63)$$

$$= h(\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{12} \quad (64)$$

where $W_{-j}^K \stackrel{\triangle}{=} \{W_i\}_{i=1,i\neq j}^K$ is the message set containing all unintended messages with respect to receiver j, $\mathbf{X}_{-j}^K \stackrel{\triangle}{=} \{\mathbf{X}_i\}_{i=1,i\neq j}^K$ and $\mathbf{Y}_{-j}^K \stackrel{\triangle}{=} \{\mathbf{Y}_i\}_{i=1,i\neq j}^K$.

For each j, we 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 a zero-mean Gaussian random variable 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 (64),

$$n\sum_{i=1,i\neq j}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{12} \quad (65)$$

$$\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{X}_1^K) - h(\mathbf{Y}_j) + nc_{12} \quad (66)$$

$$= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{N}}_1^K) - h(\mathbf{Y}_j) + nc_{12} \quad (67)$$

$$\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{13} \quad (68)$$

$$= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{13} \quad (69)$$

$$\leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{14} \quad (70)$$

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*, which is shown as follows

$$h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) \leq \sum_{j=1}^{K} h(\mathbf{Y}_j|\tilde{\mathbf{X}}_1^K) \quad (71)$$

$$= \sum_{j=1}^{K} h\left(\sum_{i=1}^{K} h_{ij}(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right) \quad (72)$$

$$= \sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right) \quad (73)$$

$$\leq \sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j\right) \tag{74}$$

$$\stackrel{\triangle}{=} nc_{15} \tag{75}$$

We apply the *role of a helper lemma*, Lemma 1, to each $\tilde{\mathbf{X}}_i$ with $k = i+1$ (for $i = K$, $k = 1$), in (70) as

$$n\sum_{i=1,i\neq j}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{14} \tag{76}$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_j) + nc_{14} \tag{77}$$

$$\leq \sum_{i=1}^{K-1}\Big[h(\mathbf{Y}_{i+1}) - nR_{i+1}\Big] + \Big[h(\mathbf{Y}_1) - nR_1\Big] - h(\mathbf{Y}_j) + nc_{16} \tag{78}$$

$$= \sum_{i=1}^{K}\Big[h(\mathbf{Y}_i) - nR_i\Big] - h(\mathbf{Y}_j) + nc_{16} \tag{79}$$

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

$$nR_j + 2n\sum_{i=1,i\neq j}^{K} R_i \leq \sum_{i=1,i\neq j}^{K} h(\mathbf{Y}_i) + nc_{16} \tag{80}$$

$$\leq (K-1)\left(\frac{n}{2}\log P\right) + nc_{17} \tag{81}$$

for $j = 1,\ldots,K$. Therefore, we have a total of K bounds in (81) for $j = 1,\ldots,K$. Summing these K bounds, we obtain:

$$(2K-1)n\sum_{i=1}^{K} R_i \leq K(K-1)\left(\frac{n}{2}\log P\right) + nc_{18} \tag{82}$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{83}$$

completing the converse for IC-CM.

VI. Achievability

In this section, we provide achievability for the K-user IC-CM-EE (see Fig. 2(c)), which will imply achievability for K-user IC-EE and K-user IC-CM. We will prove that, for almost all channel gains, a sum secure d.o.f. lower bound of

$$D_{s,\Sigma} \geq \frac{K(K-1)}{2K-1} \tag{84}$$

is achievable for the K-user IC-CM-EE.

A. Background

In this section, we will summarize the achievability scheme for the two-user IC-CM in [38], motivate the need for simultaneous alignment of multiple signals at multiple receivers in this K-user case, and provide an example of simultaneously aligning two signals at two receivers via asymptotic real alignment [44]. We provide the general achievable scheme for $K > 2$ in Section VI-B via cooperative jamming and asymptotic real alignment, and show that it achieves the sum secure d.o.f. in (84) via a detailed performance analysis in Section VI-C.

In the achievable scheme for $K = 2$ in [38], four mutually independent discrete random variables $\{V_1, U_1, V_2, U_2\}$ are employed (see [38, Fig. 10]). Each of them is uniformly and independently drawn from the discrete constellation $C(a, Q)$ given in (10). The role of V_i is the signal carrying 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 at receiver 1, and U_2 and V_1 are aligned 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,

$$V_{ij}, \quad i, j = 1,\ldots,K,\ j \neq i \tag{85}$$

$$U_k, \quad k = 1,\ldots,K \tag{86}$$

which are illustrated in Fig. 3 for the case of $K = 3$. The scheme proposed here has two major differences from [38]: 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 $\{V_{ik}\}_{i\neq k, i\neq j}$ at receivers j, and at the eavesdropper (if there is any). For example, in Fig. 3, 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 particular alignments are circled by ellipsoids in Fig. 3. We do these simultaneous alignments using asymptotic real alignment technique proposed in [44] and used in [30] and [36].[4]

For illustration purposes, in the rest of this section, we demonstrate how we can align two signals at two receivers simultaneously; in particular, we will align U_1 with V_{21} at Y_1 and Y_3, simultaneously. Towards this end, we will further divide the random variable V_{21}, which represents a sub-message, into a large number of random variables denoted as $V_{21} \stackrel{\triangle}{=} \{v_{21t} : t = 1,\ldots,|T_1|\}$. We then send each one of these random variables after multiplying it with one of the coefficients in the following set which serves as the set of

[4]The achievability scheme developed in this paper relies on the perfect knowledge of the channel state information (CSI) of all channels at all terminals. References [39], [40] developed a *blind cooperative jamming* scheme that utilizes only the legitimate receiver's CSI. In particular, [40] achieved the optimum secure d.o.f. (i.e., secure d.o.f. with complete CSI of all terminals) by using only the legitimate receiver's CSI in a helper network. Extension of such schemes to an interference network is an open problem.

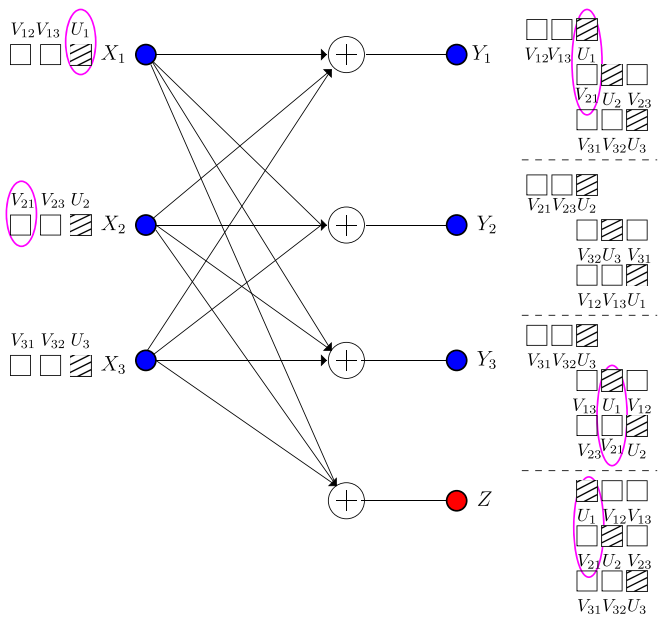

Fig. 3. Illustration of alignment for 3-user IC-CM-EE. U_1 and V_{21} are marked to emphasize their simultaneous alignment at Y_1, Y_3 and Z.

dimensions:

$$T_1 = \left\{ h_{11}^{r_{11}} h_{21}^{r_{21}} h_{13}^{r_{13}} h_{23}^{r_{23}} : \; r_{11}, r_{21}, r_{13}, r_{23} \in \{1, \ldots, m\} \right\} \quad (87)$$

where m is a very large constant. To perform the alignment, we let U_1 have the same detailed structure as V_{21}, i.e., U_1 is also divided into a large number of random variables as $U_1 \triangleq \{u_{1t} : t = 1, \ldots, |T_1|\}$. 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.,

$$|h_{11}T_1 \cap h_{21}T_1| = m^2(m-1)^2 \approx m^4 = |T_1| \quad (88)$$

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 for receiver 3. At receiver 3, the elements of U_1 from transmitter 1 occupy the dimensions $h_{13}T_1$ and the elements of V_{21} from transmitter 2 occupy the dimensions $h_{23}T_1$. Again, although these two sets are not the same, their intersection contains nearly as many elements as T_1. Therefore, almost all elements of U_1 and V_{21} are aligned at receivers 1 and 3, simultaneously. These simultaneous alignments are depicted in Fig. 4. In the following section, we use this basic idea to align multiple signals at multiple receivers simultaneously. This will require a more intricate design of signals and dimensions.

B. General Achievable Scheme via Asymptotic Alignment

Here, we give the general achievable scheme for the K-user IC-CM-EE. Let m be a large constant. Let us define sets T_i, for $i = 1, \ldots, K$, which will represent *dimensions* as follows:

$$T_i \triangleq \left\{ h_{ii}^{r_{ii}} \left(\prod_{j,k=1, j\neq k}^{K} h_{jk}^{r_{jk}} \right) \left(\prod_{j=1}^{K} g_j^{s_j} \right) : \right. \\ \left. r_{ii}, r_{jk}, s_j \in \{1, \ldots, m\} \right\} \quad (89)$$

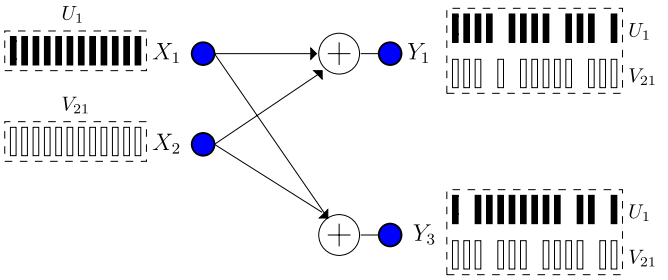

Fig. 4. Illustration of alignment at multiple receivers.

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

$$M \triangleq m^{1+K(K-1)+K} = m^{K^2+1} \quad (90)$$

For each transmitter i, for $j \neq i$, let $\mathbf{t}_{ij}$ be the vector containing all the elements in the set T_j. Therefore, $\mathbf{t}_{ij}$ is an M-dimensional vector containing M rationally independent real numbers in T_j. The sets $\mathbf{t}_{ij}$ will represent the *dimensions* along which message signals are transmitted. In particular, for any given (i, j) with $i \neq j$, $\mathbf{t}_{ij}$ will represent the dimensions in which message signal V_{ij} is transmitted. In addition, for each transmitter i, let $\mathbf{t}_{(i)}$ be the vector containing all the elements in the set T_i. Therefore, $\mathbf{t}_{(i)}$ is an M-dimensional vector containing M rationally independent real numbers in T_i. The sets $\mathbf{t}_{(i)}$ will represent the *dimensions* along which cooperative jamming signals are transmitted. In particular, for any given i, $\mathbf{t}_{(i)}$ will represent the dimensions in which cooperative jamming signal U_i is transmitted. Let us define a KM dimensional vector $\mathbf{b}_i$ by stacking $\mathbf{t}_{ij}$ and $\mathbf{t}_{(i)}$ as

$$\mathbf{b}_i^T = \left[\mathbf{t}_{i1}^T, \ldots, \mathbf{t}_{i,i-1}^T, \mathbf{t}_{i,i+1}^T, \ldots, \mathbf{t}_{iK}^T, \mathbf{t}_{(i)}^T \right] \quad (91)$$

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

$$\mathbf{a}_i^T = \left[\mathbf{v}_{i1}^T, \ldots, \mathbf{v}_{i,i-1}^T, \mathbf{v}_{i,i+1}^T, \ldots, \mathbf{v}_{iK}^T, \mathbf{u}_i^T \right] \quad (92)$$

where $\mathbf{v}_{ij}$ represents the information symbols in V_{ij}, and $\mathbf{u}_i$ represents the cooperative jamming signal in U_i. Each of these vectors has length M, and therefore, the total length of $\mathbf{a}_i$ is KM. The channel input of transmitter i is

$$x_i = \mathbf{a}_i^T \mathbf{b}_i \quad (93)$$

Before we investigate the performance of this signalling scheme in Section VI-C, we analyze the structure of the received signal at the receivers. Without loss of generality we will focus on receiver 1; by symmetry, a similar structure will exist at all other receivers. We observe that in addition to the additive Gaussian noise, receiver 1 receives all the vectors $\mathbf{v}_{jk}$ for all $j, k\,(j \neq k)$ and $\mathbf{u}_i$ for all i. All of these signals get multiplied with the corresponding channel gains before they arrive at receiver 1. Due to the specific signalling structure used at the transmitters, and the multiplications with different channel gains over the wireless communication channel, the signals arrive at the receiver lying in various different *dimensions*.

To see the detailed structure of the received signals at the receivers, let us define $\tilde{T}_i$ as a superset of T_i, as follows

$$\tilde{T}_i \triangleq \left\{ h_{ii}^{r_{ii}} \left(\prod_{j,k=1, j\neq k}^{K} h_{jk}^{r_{jk}} \right) \left(\prod_{j=1}^{K} g_j^{s_j} \right) : r_{ii}, r_{jk}, s_j \in \{1, \ldots, m+1\} \right\} \quad (94)$$

The information symbols coming from transmitter 1 are in vectors $\mathbf{v}_{12}, \mathbf{v}_{13}, \ldots, \mathbf{v}_{1K}$ which are multiplied by coefficients in $\mathbf{t}_{12}, \mathbf{t}_{13}, \ldots, \mathbf{t}_{1K}$ before they are sent. These coefficients come from sets $T_2, T_3, \ldots, T_K$, respectively. After going through the channel, all of these coefficients get multiplied by h_{11}. Therefore, the receiving coefficients of $\mathbf{v}_{12}, \mathbf{v}_{13}, \ldots, \mathbf{v}_{1K}$ are $h_{11}\mathbf{t}_{12}, h_{11}\mathbf{t}_{13}, \ldots, h_{11}\mathbf{t}_{1K}$, which are the *dimensions* in the sets $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K$, respectively. By construction, since each T_i has powers of h_{ii} in it (but no h_{jj}), these dimensions are *separate* almost surely. These correspond to *separate* boxes of V_{12} and V_{13} at receiver 1 in Fig. 3 for the example case of $K = 3$.

On the other hand, all of the cooperative jamming signals from all of the transmitters $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K$ come to receiver 1 with received coefficients $h_{11}\mathbf{t}_{(1)}, h_{21}\mathbf{t}_{(2)}, \ldots, h_{K1}\mathbf{t}_{(K)}$, which are the *dimensions* in the sets $h_{11}T_1, h_{21}T_2, \ldots, h_{K1}T_K$, respectively. We note that almost surely all of these dimensions are separate among themselves, and they are separate from the dimensions of the message signals coming from transmitter 1. That is, all of the dimensions in $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K$ and $h_{11}T_1, h_{21}T_2, \ldots, h_{K1}T_K$ are all mutually different, again owing to the fact that each T_i contains powers of h_{ii} in it. These correspond to separate boxes of V_{12}, V_{13}, U_1, U_2 and U_3 at receiver 1 in Fig. 3 for the example case of $K = 3$.

Next, we note that each $\mathbf{u}_i$ is aligned together with all of the $\mathbf{v}_{ji}$ coming from the jth transmitter, with $j \neq i$ and $j \neq 1$, at receiver 1. Note that $\mathbf{u}_i$ occupies dimensions $h_{i1}T_i$ and $\mathbf{v}_{ji}$ (for any $j \neq i$ and $j \neq 1$) occupies dimensions $h_{j1}T_i$ at receiver 1. From the arguments in Section VI-A, $\mathbf{u}_i$ and $\mathbf{v}_{ji}$ (with $j \neq i$ and $j \neq 1$) are asymptotically aligned. More formally, we note that $\mathbf{u}_i$ occupies dimensions $h_{i1}T_i$ which is contained in $\tilde{T}_i$. Similarly, all $\mathbf{v}_{ji}$, with $j \neq i$ and $j \neq 1$, occupy dimensions $h_{j1}T_i$, respectively, which are all contained in $\tilde{T}_i$. Therefore, $\mathbf{u}_i$ and all $\mathbf{v}_{ji}$ (with $j \neq i$ and $j \neq 1$) are all aligned along $\tilde{T}_i$. These alignments are shown as U_1 being aligned with V_{21} and V_{31}; U_2 being aligned with V_{32}; and U_3 being aligned with V_{23} at receiver 1 in Fig. 3 for the example case of $K = 3$. Further, we note that, since only T_i and $\tilde{T}_i$ contain powers of h_{ii}, the dimensions $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K, \tilde{T}_1, \tilde{T}_2, \ldots, \tilde{T}_K$ are all separable. This implies that all the elements in the set

$$S_1 \triangleq \left(\bigcup_{j=2}^{K} h_{11}T_j \right) \bigcup \left(\bigcup_{j=2}^{K} \tilde{T}_j \right) \bigcup \tilde{T}_1 \quad (95)$$

are rationally independent, and thereby the cardinality of S_1 is

$$\begin{aligned} M_S &\triangleq |S_1| && (96)\\ &= (K-1)m^{1+K(K-1)+K} + K(m+1)^{1+K(K-1)+K} && (97)\\ &= (K-1)m^{K^2+1} + K(m+1)^{K^2+1} && (98) \end{aligned}$$

C. Performance Analysis

We will compute the secrecy rates achievable with the asymptotic alignment based scheme proposed in Section VI-B by using the following theorem.

Theorem 2: For K-user interference channels with confidential messages and one external eavesdropper, the following rate region is achievable

$$R_i \geq I(V_i; Y_i) - \max_{j \in \mathcal{K}_{0,-i}} I(V_i; Y_j | V_{-i}^K), \quad i = 1, \ldots, K \quad (99)$$

where for convenience we denote Z by Y_0, $V_{-i}^K \triangleq \{V_j\}_{j=1, j\neq i}^K$ and $\mathcal{K}_{0,-i} = \{0, 1, \ldots, i-1, i+1, \ldots, K\}$. The auxiliary random variables $\{V_i\}_{i=1}^K$ are mutually independent, and for each i, we have the following Markov chain $V_i \rightarrow X_i \rightarrow (Y_0, Y_1, \ldots, Y_K)$.

In developing the achievable rates in Theorem 2, we focus on a single transmitter, say i, and consider the compound setting associated with message W_i, where this message needs to be secured against a total of K eavesdroppers, with $K-1$ of them being the other legitimate receivers ($j \neq i$) and the remaining one being the external eavesdropper ($j = 0$). A proof of this theorem is given in Appendix.

We apply Theorem 2 to our alignment based scheme proposed in Section VI-B by selecting V_i used in (99) as

$$V_i \triangleq (\mathbf{v}_{i1}^T, \ldots, \mathbf{v}_{i,i-1}^T, \mathbf{v}_{i,i+1}^T, \ldots, \mathbf{v}_{iK}^T) \quad (100)$$

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

$$\Pr(V_i \neq \hat{V}_i) \leq \exp\left(-\eta_{\gamma_i} P^{\delta}\right) \quad (101)$$

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

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

$$\begin{aligned} I(V_i; Y_i) &\geq I(V_i; \hat{V}_i) && (102)\\ &= H(V_i) - H(V_i|\hat{V}_i) && (103)\\ &= \log(|\mathcal{V}_i|) - H(V_i|\hat{V}_i) && (104)\\ &\geq \log(|\mathcal{V}_i|) - 1 - \Pr(V_i \neq \hat{V}_i)\log(|\mathcal{V}_i|) && (105)\\ &= \left[1 - \Pr(V_i \neq \hat{V}_i)\right]\log(|\mathcal{V}_i|) - 1 && (106)\\ &= \log(|\mathcal{V}_i|) - o(\log P) && (107)\\ &= \frac{(K-1)m^{K^2+1}(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (108)\\ &= \frac{(K-1)(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) && (109) \end{aligned}$$

where $o(\cdot)$ is the little-o function, $\mathcal{V}_i$ is the alphabet of V_i and, in this case, the cardinality of $\mathcal{V}_i$

is $(2Q+1)^{(K-1)M} = (2Q+1)^{(K-1)m^{K^2+1}}$. Here, M is defined in (90). This provides a lower bound for the first term in (99).

Next, we need to derive an upper bound for the second item in (99), i.e, the secrecy penalty. For any $i \in \mathcal{K} = \{1, \ldots, K\}$ and $j \in \mathcal{K}_{-i} = \{1, \ldots, i-1, i+1, \ldots, K\}$, by the Markov chain $V_i \to (\sum_{k=1}^{K} h_{kj} X_{kj}, V_{-i}^K) \to Y_j$,

$$I(V_i; Y_j | V_{-i}^K) \le I\left(V_i; \sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) \tag{110}$$

$$= H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) - H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_1^K\right) \tag{111}$$

where $V_1^K = \{V_1, \ldots, V_K\}$. The first term in (111) can be rewritten as

$$H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) = H\left(\sum_{k=1}^{K} h_{kj} \mathbf{u}_k^T \mathbf{t}_{(k)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} h_{ij} \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right) \tag{112}$$

$$= H\left(h_{ij} \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[h_{ij} \mathbf{v}_{ik}^T \mathbf{t}_{ik} + h_{kj} \mathbf{u}_k^T \mathbf{t}_{(k)}\right]\right) \tag{113}$$

Note that, for a given k, the vectors $\mathbf{t}_{ik}$ and $\mathbf{t}_{(k)}$ represent the same *dimensions* T_k, and $h_{ij}, h_{kj} \in T_k$ for all $k \neq i$, which implies that $h_{ij} T_k, h_{kj} T_k \in \tilde{T}_k$. In addition, for each k, we note that a large part of the two sets $h_{ij} T_k$ and $h_{kj} T_k$ are the same, i.e.,

$$\left|h_{ij} T_k \bigcap h_{kj} T_k\right| = m^{K^2-1}(m-1)^2 \triangleq M_\delta \tag{114}$$

Therefore, the first term in (111) can be further upper bounded as

$$H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) = H\left(h_{ij} \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[h_{ij} \mathbf{v}_{ik}^T \mathbf{t}_{ik} + h_{kj} \mathbf{u}_k^T \mathbf{t}_{(k)}\right]\right) \tag{115}$$

$$\le \log\Big[(2Q+1)^M (4Q+1)^{(K-1)M_\delta} \times (2Q+1)^{2(K-1)(M-M_\delta)}\Big] \tag{116}$$

$$\le \log\left[Q^{M+(K-1)M_\delta+2(K-1)(M-M_\delta)}\right] + o(\log P) \tag{117}$$

$$\le \left\{\frac{[M+(K-1)M_\delta+2(K-1)(M-M_\delta)](1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta} \times \left(\frac{1}{2}\log P\right)\right\} + o(\log P) \tag{118}$$

which implies that the first term in (111) can be upper bounded by (119) (on bottom of the page).

The second term in (111) is exactly the entropy of $\{\mathbf{u}_k\}_{k=1}^K$ vectors, i.e.,

$$H\left(\sum_{k=1}^{K} h_{kj} X_k | V_1^K\right) = H\left(\sum_{k=1}^{K} h_{kj} \mathbf{u}_k^T \mathbf{t}_{(k)}\right) \tag{120}$$

$$= \log(2Q+1)^{KM} \tag{121}$$

$$= \frac{Km^{K^2+1}(1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{122}$$

$$= \frac{K(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{123}$$

where (121) is true for almost all channel gains.

Substituting (119) and (123) into (111), we get

$$I(V_i; Y_j | V_{-i}^K) \le H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) - H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_1^K\right) \tag{124}$$

$$\le \frac{K\,\frac{2m-1}{m^2}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{125}$$

We note that by choosing m large enough, the factor before the $\frac{1}{2}\log P$ term 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 [38], but a function which can be made to approach zero d.o.f.

For any $i \in \mathcal{K}$ and $j = 0$, i.e., $Y_0 = Z$ the external eavesdropper, we should derive a new upper bound for the second term in (111), i.e., $I(V_i; Z | V_{-i}^K)$. By similar steps, we have

$$I(V_i; Z | V_{-i}^K) \le I\left(V_i; \sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) \tag{126}$$

$$= H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) - H\left(\sum_{k=1}^{K} g_k X_k \Big| V_1^K\right) \tag{127}$$

$$= H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) - H\left(\sum_{k=1}^{K} g_k \mathbf{u}_k^T \mathbf{t}_{(k)}\right) \tag{128}$$

$$= H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) - \log(2Q+1)^{KM} \tag{129}$$

$$H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) \le \frac{\left\{1+(K-1)\left(1-\frac{1}{m}\right)^2+2(K-1)\left[1-\left(1-\frac{1}{m}\right)^2\right]\right\}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{119}$$

where (129) is true for almost all channel gains. Here, we need to upper bound the first item in (129). We first observe that

$$H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) = H\left(\sum_{k=1}^{K} g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right) \quad (130)$$

$$= H\left(g_i \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right]\right) \quad (131)$$

Firstly, note that, $\mathbf{t}_{(k)}$ and $\mathbf{t}_{ik}$ represent the same set T_k. Therefore, for different k, the *dimensions* are distinguishable. Secondly, due to reasons similar to (114), we conclude that

$$H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) = H\left(g_i \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right]\right) \quad (132)$$

$$\leq \log\Big[(2Q+1)^M (4Q+1)^{(K-1)M_\delta} \times (2Q+1)^{2(K-1)(M-M_\delta)}\Big] \quad (133)$$

$$\leq \log\left[Q^{M+(K-1)M_\delta+2(K-1)(M-M_\delta)}\right] + o(\log P) \quad (134)$$

$$\leq \left\{\frac{[M+(K-1)M_\delta+2(K-1)(M-M_\delta)](1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta} \times \left(\frac{1}{2}\log P\right)\right\} + o(\log P) \quad (135)$$

Substituting (135) into (129), we attain an upper bound which is the same as the upper bound for $I(V_i; Y_j|V_{-i}^K)$, i.e.,

$$I(V_i; Z|V_{-i}^K) \leq \frac{K\,\frac{2m-1}{m^2}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (136)$$

Substituting (109), (125), and (136) into (99), we obtain a lower bound for the achievable secrecy rate R_i as

$$R_i \geq \frac{\left[(K-1)-K\left(\frac{2m-1}{m^2}\right)\right](1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (137)$$

By choosing $m \to \infty$ and $\delta \to 0$, we can achieve secrecy sum rates arbitrarily close to $\frac{K-1}{2K-1}\left(\frac{1}{2}\log P\right)$, thereby achieving the sum secure d.o.f. lower bound in (84).

VII. Conclusion

In this paper, we studied secure communications in K-user Gaussian interference networks from an information-theoretic point of view, and addressed three important channel models: IC-EE, IC-CM and their combination IC-CM-EE in a unified framework. We showed that, for all three models, the sum secure d.o.f. is exactly $\frac{K(K-1)}{2K-1}$. Our achievability is based on structured signalling, structured cooperative jamming, channel prefixing and asymptotic real interference alignment. The key insight of the achievability is to carefully design the structure of all of the signals at the transmitters so that the signals are received at both legitimate receivers and eavesdroppers in most desirable manner from a secure communication point of view. In particular, cooperative jamming signals protect information carrying signals via alignment, and the information carrying signals are further aligned to maximize secure d.o.f.

Appendix

We first provide an outline of the proof. Our proof will combine and extend techniques from [5] and [26]. Our approach has three main components. First, as in [5], we condition the mutual information representing the secrecy leakage rate on the signals that carry the messages of other transmitter-receiver pairs. That is, for any given i, we condition the subtracted mutual information term in (99) on V_{-i}^K. This creates *enhanced* eavesdroppers. If we can guarantee secrecy against these enhanced eavesdroppers, we can guarantee secrecy against the original eavesdroppers. More specifically, for the leakage rate of message of transmitter i at receiver j, with $j \neq i$, we use

$$I(V_i; Y_j|V_{-i}^K) = I(V_i; Y_j, V_{-i}^K) \stackrel{\triangle}{=} I(V_i; \tilde{Y}_j) \quad (138)$$

where $\tilde{Y}_j \stackrel{\triangle}{=} (Y_j, V_{-i}^K)$ is the output of an *enhanced* eavesdropper with respect to message W_i. Second, as in [26], we consider the secrecy rate achievable against the *strongest* enhanced eavesdropper for each message. Therefore, as argued in [26, Appendix A], if we can guarantee a secrecy rate against the strongest eavesdropper, we can guarantee this secrecy rate against the original eavesdroppers. More specifically, let $Y^{(i)}$ be an element of the set $\{Y_1, \ldots, Y_k, Z\}\backslash\{Y_i\}$ such that

$$I(V_i; Y^{(i)}|V_{-i}^K) = \max_{j\in\mathcal{K}_{0,-i}} I(V_i; Y_j|V_{-i}^K) \quad (139)$$

That is, $Y^{(i)}$ is the *strongest* eavesdropper with respect to transmitter i. The achievable rate in (99) considers the strongest eavesdropper for each message. Therefore, for each transmitter i, we construct a compound wiretap code as in [26]. Third, we prove secrecy for each message W_i, via the following equivocation inequality

$$H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) \geq H(W_i) - n\epsilon^{(i)}, \quad i = 1, \ldots, K \quad (140)$$

for some arbitrarily small number $\epsilon^{(i)}$. Here, as in the main body of the paper, we denote n-length sequences with boldface letters. The secrecy constraints in (140) fit the created equivalent view of the channel better. As we show next, secrecy constraints in (140) imply our original secrecy constraints in (4) and (5).

Towards this end, first note that, for each i,

$$H(W_i|\mathbf{Y}_j, \mathbf{V}_{-i}^K) \geq H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) \geq H(W_i) - n\epsilon^{(i)} \quad (141)$$

for all $j \in \mathcal{K}_{0,-i}$ since $Y^{(i)}$ is the *strongest* eavesdropper with respect to transmitter i and by using the enhanced

eavesdropper argument in [26, Appendix A]. Then, the fact that (140) for all i implies the original secrecy constraints in (4) and (5) follows from the following derivation:

$$\begin{aligned} H(W_{-j}^K|\mathbf{Y}_j) &\geq H(W_{-j}^K|\mathbf{Y}_j, W_j) && (142)\\ &\geq \sum_{i\neq j} H(W_i|\mathbf{Y}_j, W_{-i}^K) && (143)\\ &\geq \sum_{i\neq j} H(W_i|\mathbf{Y}_j, \mathbf{V}_{-i}^K, W_{-i}^K) && (144)\\ &= \sum_{i\neq j} H(W_i|\mathbf{Y}_j, \mathbf{V}_{-i}^K) && (145)\\ &\geq \sum_{i\neq j} H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) && (146)\\ &\geq \sum_{i\neq j} \left[H(W_i) - n\epsilon^{(i)}\right] && (147)\\ &= H(W_{-j}^K) - n\epsilon^{(-j)} && (148) \end{aligned}$$

where (145) is due to the Markov chain $W_{-i}^K \rightarrow (\mathbf{Y}_j, \mathbf{V}_{-i}^K) \rightarrow W_i$. Similarly,

$$\begin{aligned} H(W^K|\mathbf{Z}) &\geq \sum_i H(W_i|\mathbf{Z}, W_{-i}^K) && (149)\\ &\geq \sum_i H(W_i|\mathbf{Z}, \mathbf{V}_{-i}^K, W_{-i}^K) && (150)\\ &= \sum_i H(W_i|\mathbf{Z}, \mathbf{V}_{-i}^K) && (151)\\ &\geq \sum_i H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) && (152)\\ &\geq \sum_i \left[H(W_i) - n\epsilon^{(i)}\right] && (153)\\ &= H(W^K) - n\epsilon^{(Z)} && (154) \end{aligned}$$

where $\epsilon^{(Z)}$ is small for sufficiently large n.

We start by choosing the following rates for the secure and confusion messages of transmitter i:

$$\begin{aligned} R_i &= I(V_i; Y_i) - I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon && (155)\\ R_i^c &= I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon && (156) \end{aligned}$$

Transmitter i generates $2^{n(R_i+R_i^c)}$ independent sequences each with probability

$$p(\mathbf{v}_i) = \prod_{t=1}^{n} p(v_{it}) \tag{157}$$

and constructs a codebook as

$$C_i \triangleq \left\{\mathbf{v}_i(w_i, w_i^c) \,:\, w_i \in \{1, \ldots, 2^{nR_i}\}, w_i^c \in \{1, \ldots, 2^{nR_i^c}\}\right\} \tag{158}$$

To transmit a message w_i, transmitter i chooses an element $\mathbf{v}_i$ from the sub-codebook $C_i(w_i)$

$$C_i(w_i) \triangleq \left\{\mathbf{v}_i(w_i, w_i^c) \,:\, w_i^c \in \{1, \ldots, 2^{nR_i^c}\}\right\} \tag{159}$$

and generates a channel input sequence based on

$$p(x_i|v_i) \tag{160}$$

Due to the code construction, we have $R_i + R_i^c < I(V_i; Y_i)$, for all i. Therefore, for sufficiently large n_i, we can find a codebook such that the probability of error at the corresponding receiver i can be upper bounded by an arbitrarily small number, i.e., $\Pr(e_i)^{(n_i)} \leq \epsilon$. Then, let $n = \max_i n_i$, which gives $\max_i \Pr(e_i)^{(n)} \leq \epsilon$.

For the equivocation calculation, we consider the following conditional entropy as discussed before:

$$\begin{aligned} &H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K)\\ &\quad= H(W_i, \mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) && (161)\\ &\quad= H(W_i, \mathbf{V}_i, \mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) - H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K)\\ &\qquad- H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) && (162)\\ &\quad= H(W_i, \mathbf{V}_i|\mathbf{V}_{-i}^K) + H(\mathbf{Y}^{(i)}|W_i, \mathbf{V}_i, \mathbf{V}_{-i}^K)\\ &\qquad- H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) && (163)\\ &\quad= H(W_i, \mathbf{V}_i|\mathbf{V}_{-i}^K) - H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K)\\ &\qquad+H(\mathbf{Y}^{(i)}|\mathbf{V}_i, \mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) && (164) \end{aligned}$$

where the last equality is due to the Markov chain $W_i \rightarrow (\mathbf{V}_i, \mathbf{V}_{-i}^K) \rightarrow \mathbf{Y}^{(i)}$.

The first term in (164) is exactly the entropy of codebook C_i:

$$H(\mathbf{V}_i) = n(R_i + R_i^c) \tag{165}$$

To bound the second term in (164), we have the following observation: Given the message $W_i = w_i$ and the received sequences $\mathbf{Y}^{(i)} = \mathbf{y}^{(i)}$ and genie-aided sequences $\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K$, receiver $Y^{(i)}$ can decode the codeword $\mathbf{v}_i(w_i, w_i^c)$ with arbitrarily small probability of error $\lambda(w_i)^{(n)}$ as n gets very large. More formally: by giving $W_i = w_i, \mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K$, receiver $Y^{(i)}$ decodes $\mathbf{V}_i$ if there is a unique w_i^c such that

$$\left(\mathbf{v}_i(w_i, w_i^c), \mathbf{y}^{(i)}\right) \in T_\epsilon^{(n)}(P_{V_1, Y^{(i)}|V_{-i}^K})(\mathbf{v}_{-i}^K) \tag{166}$$

Otherwise, the receiver declares an error. Without loss of generality, we assume that $\mathbf{v}_i(w_i, w_1^c)$ is sent and denote the event $\left\{(\mathbf{v}_i(w_i, w_j^c), \mathbf{y}^{(i)}) \in T_\epsilon^{(n)}(P_{V_1, Y^{(i)}|V_{-i}^K})(\mathbf{v}_{-i}^K)\right\}$ as E_j. Therefore, the probability of error $\lambda(w_i)^{(n)}$ can be bounded as

$$\lambda(w_i)^{(n)} \leq \Pr(E_1^c) + \sum_{j\neq 1} \Pr(E_j) \tag{167}$$

where the probability here is conditioned on the event that $\mathbf{v}_i(w_i, w_1^c)$ is sent. By joint typicality, we know that $\Pr(E_1^c) \leq \epsilon_1$ for sufficiently large n, and

$$\begin{aligned} \Pr(E_j) &\leq 2^{nH(V_i, Y^{(i)}|V_{-i}^K) - nH(V_i) - nH(Y^{(i)}|V_{-i}^K) - n\epsilon_2}\\ &= 2^{-nI(V_I; Y^{(i)}|V_{-i}^K) - n\epsilon_2} && (168) \end{aligned}$$

where $\epsilon_1, \epsilon_2, \ldots$ in this section are small positive numbers for sufficiently large n.

Hence,

$$\lambda(w_i)^{(n)} \leq \epsilon_1 + 2^{nR_i^c} 2^{-nI(V_I; Y^{(i)}|V_{-i}^K) - n\epsilon_2} \tag{169}$$

Note that $R_i^c = I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon$. Therefore, we can conclude that $\lambda(w_i)^{(n)} \leq \epsilon_3$ for sufficiently large n, which

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_i,\mathbf{V}_{-i}^K)=\sum_{\mathbf{v}_i,\mathbf{v}_{-i}^K}\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)}|\mathbf{V}_i=\mathbf{v}_i,\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \tag{171}$$

$$\geq\sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\left[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)}|\mathbf{V}_i=\mathbf{v}_i,\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)\right] \tag{172}$$

$$\geq\sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\Bigg[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)\sum_{(a,b)\in\mathcal{V}_i\times\mathcal{V}_{-i}^K}N(a,b|\mathbf{v}_i,\mathbf{v}_{-i}^K)\sum_{y^{(i)}\in\mathcal{Y}^{(i)}}-p(y^{(i)}|a,b)\log p(y^{(i)}|a,b)\Bigg] \tag{173}$$

$$\geq\sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\Bigg[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)\sum_{(a,b)\in\mathcal{V}_i\times\mathcal{V}_{-i}^K}n\Big(\Pr(V_i=a,V_{-i}^K=b)-\epsilon_5\Big)\sum_{y^{(i)}\in\mathcal{Y}^{(i)}}-p(y^{(i)}|a,b)\log p(y^{(i)}|a,b)\Bigg] \tag{174}$$

$$\geq\sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}n\Big[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(Y^{(i)}|V_i,V_{-i}^K)-\epsilon_6\Big] \tag{175}$$

$$\geq(1-\epsilon_7)nH(Y^{(i)}|V_i,V_{-i}^K)-n\epsilon_8 \tag{176}$$

$$\geq nH(Y^{(i)}|V_i,V_{-i}^K)-n\epsilon_9 \tag{177}$$

by Fano's inequality further implies that

$$H(\mathbf{V}_i|W_i,\mathbf{Y}^{(i)},\mathbf{V}_{-i}^K)\leq\Big(1+\lambda(w_i)^{(n)}\log 2^{n(R_i+R_i^c)}\Big)\leq n\epsilon_4 \tag{170}$$

The third term in (164) can be lower bounded as in (177) (on top of the page).

To compute the forth term in (164), we define

$$\hat{\mathbf{Y}}^{(i)}=\begin{cases}\mathbf{Y}^{(i)}, & \text{if } (\mathbf{v}_{-i}^K,\mathbf{y}^{(i)})\in T_\epsilon^{(n)}(P_{V_{-i}^K,Y^{(i)}})\\ \text{arbitrary}, & \text{otherwise}\end{cases} \tag{178}$$

Then, we obtain

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K)=\sum_{\mathbf{v}_{-i}^K}\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \tag{179}$$

$$\leq\sum_{\mathbf{v}_{-i}^K}\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)},\hat{\mathbf{Y}}^{(i)}|\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \tag{180}$$

$$=\sum_{\mathbf{v}_{-i}^K}\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)\Big[H(\hat{\mathbf{Y}}^{(i)}|\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)+H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K,\hat{\mathbf{Y}}^{(i)})\Big] \tag{181}$$

$$\leq nH(Y^{(i)}|V_{-i}^K)+n\epsilon_1+\sum_{\mathbf{v}_{-i}^K}\Big[\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K,\hat{\mathbf{Y}}^{(i)})\Big] \tag{182}$$

Combining Fano's inequality and the fact that

$$\Pr(\mathbf{Y}^{(i)}\neq\hat{\mathbf{Y}}^{(i)})\leq\Pr\Big\{(\mathbf{V}_{-i}^K,\mathbf{Y}^{(i)})\notin T_\epsilon^{(n)}(P_{V_{-i}^K,Y^{(i)}})\Big\} \tag{183}$$

is arbitrarily small for sufficiently large n, (182) implies

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K)\leq nH(Y^{(i)}|V_{-i}^K)+n\epsilon_1+n\epsilon_2 \tag{184}$$

Substituting (165), (170), (178), and (184) into (164), we conclude that

$$H(W_i|\mathbf{Y}^{(i)},\mathbf{V}_{-i}^K)\geq H(W_i)-n\epsilon^{(i)} \tag{185}$$

where $\epsilon^{(i)}$ is small for sufficiently large n, 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, Jan. 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. 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. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[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.*, Mar. 2009, Art. ID 824235.

[11] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *J. Commun. Netw.*, vol. 12, no. 5, pp. 411–432, Oct. 2010.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] E. Ekrem and S. Ulukus, "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.

[19] 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.

[20] Y. Oohama. (Nov. 2006). "Relay channels with confidential messages." [Online]. Available: http://arxiv.org/abs/cs/0611125

[21] 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.

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

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

[24] 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.

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

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

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

[28] 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.

[29] 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.

[30] 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./Oct. 2010, pp. 1252–1257.

[31] 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.

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

[33] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. (Mar. 2010). "On the secure degrees-of-freedom of the multiple-access-channel." [Online]. Available: http://arxiv.org/abs/1003.0729

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

[35] 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.

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

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

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

[44] 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.

[45] T. Gou, S. A. Jafar, C. Wang, S.-W. Jeon, and S.-Y. Chung, "Aligned interference neutralization and the degrees of freedom of the $2 \times 2 \times 2$ interference channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4381–4395, Jul. 2012.

[46] 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.

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

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) 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 communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, 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 *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 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.