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

Jianwei Xie  Sennur Ulukus

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu  ulukus@umd.edu

May 31, 2013

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 of the interfered users, and by quantifying the secrecy penalty in terms of the eavesdroppers’ observations. Our achievability uses 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 sub-space 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.

*This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.
# 1 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 [28–40]. In this paper, we focus on the $K$-user interference channel with secrecy constraints, and determine its exact sum secure d.o.f.

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 Figure 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, see Figure 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 Figure 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 Figure 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][30] is basically to evaluate the secrecy performance of the interference alignment technique [41] 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 [41] 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 [42]. 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.

Figure 1: $K$-user Gaussian interference channel with secrecy constraints.
Figure 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 $W_{\triangleleft i} \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

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 [43], 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 $\frac{K^2}{2}$, which is the upper bound with no secrecy constraints [41]. 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.

2 System Model, Definitions and the Result

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

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

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

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 $j$th transmitter to the $i$th receiver, $g_j$ is the channel gain of the $j$th 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, $E[X_i^2] \leq P$, 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 $f_i : W_i \rightarrow X_i$ to encode the message, where $X_i \triangleq X_i^n$ is the $n$-length channel input of user $i$. We use boldface letters to denote $n$-length vector signals, e.g., $X_i \triangleq X_i^n$, $Y_j \triangleq Y_j^n$, $Z \triangleq Z^n$, etc. The legitimate receiver $j$ decodes the message as $\hat{W}_j$ based on its observation $Y_j$. 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 $\epsilon$ for all messages,

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

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

1) In IC-EE, Figure 2(a), all of the messages are kept information-theoretically secure against the external eavesdropper,

$$H(W_1, \ldots, W_K | Z) \geq H(W_1, \ldots, W_K) - n\epsilon$$

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

$$H(W^K_{-i} | Y_i) \geq H(W^K_{-i}) - n\epsilon, \quad i = 1, \ldots, K$$

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

3) In IC-CM-EE, Figure 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

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

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.
3 Preliminaries

3.1 Role of a Helper Lemma

For completeness, we repeat Lemma 2 in [38] 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 $k$th transmitter’s signal at the $k$th receiver, the channel input of transmitter $i \neq k$, $X_i$, must satisfy

$$h(X_i + \tilde{N}) \leq h(Y_k) - nR_k + nc$$

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 $\sigma^2_{\tilde{N}} < \frac{1}{h_{ik}}$, and $\tilde{N}$ 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 (7), 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, (7), 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.

3.2 Real Interference Alignment

3.2.1 Pulse Amplitude Modulation

For a point-to-point scalar Gaussian channel,

$$Y = X + Z$$

with additive Gaussian noise $Z \sim \mathcal{N}(0, \sigma^2)$ and an input power constraint $E[X^2] \leq P$, assume that the input symbols are drawn from a PAM constellation,

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

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 $d_{\text{min}}(C)$ of this constellation, which has the probability
of error
\[ \Pr(e) \leq \exp \left( -\frac{d_{\text{min}}^2}{8\sigma^2} \right) = \exp \left( -\frac{a^2}{8\sigma^2} \right) \] (10)

The transmission rate of this PAM scheme is
\[ R = \log(2Q + 1) \] (11)

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 \(\gamma\) is a constant to normalize the transmit power, which is independent of \(P\), then
\[ \Pr(e) \leq \exp \left( -\frac{\gamma^2 P^{\delta}}{8\sigma^2} \right) \quad \text{and} \quad R \geq \frac{1 - \delta}{2} \log P \] (12)

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 \(\frac{1}{2} \log P\), and therefore have 1 d.o.f.

### 3.2.2 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
\[ x = a^T \cdot b = \sum_{i=1}^{L} a_i b_i \] (13)

where \(a_1, \ldots, a_L\) are rationally independent real numbers\(^1\) and each \(b_i\) is drawn independently from the constellation \(C(a, Q)\) in (9). 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, \([12,13]\) bounded the minimum distance \(d_{\text{min}}\) of points in the receiver’s constellation: For any \(\delta > 0\), there exists a constant \(k_{\delta}\), such that
\[ d_{\text{min}} \geq \frac{k_{\delta} a}{Q^{L-1+\delta}} \] (14)

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

\(^1\) \(a_1, \ldots, a_L\) are rationally independent if whenever \(q_1, \ldots, q_L\) are rational numbers then \(\sum_{i=1}^{L} q_i a_i = 0\) implies \(q_i = 0\) for all \(i\).
Lemma 2 ([42, 43]) For any small enough \( \delta > 0 \), there exists a positive constant \( \gamma \), which is independent of \( P \), such that if we choose

\[
Q = P^{\frac{1}{2(\epsilon+\delta)}} \quad \text{and} \quad a = \gamma \frac{P_{\delta}^{\frac{1}{2}}}{Q}
\]

(15)

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

\[
\Pr(e) \leq \exp\left(-\eta_{\gamma} P^{\delta}\right)
\]

(16)

where \( \eta_{\gamma} \) is a positive constant which is independent of \( P \).

Furthermore, as a simple extension, if \( b_i \) are sampled independently from different constellations \( C_i(a, Q_i) \), the lower bound in (14) can be modified as

\[
d_{\min} \geq \frac{k_a}{(\max_i Q_i)^{L-1+\epsilon}}
\]

(17)

4 Converse for IC-EE

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

\[
n \sum_{i=1}^{K} R_i = \sum_{i=1}^{K} H(W_i) = H(W^K_1)
\]

(18)

\[
\leq I(W^K_1; Y^K_1) - I(W^K_1; Z) + nc_0
\]

(19)

\[
\leq I(W^K_1; Y^K_1, Z) - I(W^K_1; Z) + nc_0
\]

(20)

\[
= I(W^K_1, Y^K_1 | Z) + nc_0
\]

(21)

\[
\leq I(X^K_1; Y^K_1 | Z) + nc_0
\]

(22)

\[
= h(Y^K_1 | Z) - h(Y^K_1 | Z, X^K_1) + nc_0
\]

(23)

\[
= h(Y^K_1 | Z) - h(N^K_1 | Z, X^K_1) + nc_0
\]

(24)

\[
\leq h(Y^K_1 | Z) + nc_1
\]

(25)

\[
= h(Y^K_1, Z) - h(Z) + nc_1
\]

(26)

where \( W^K_1 \triangleq \{W_j\}_{j=1}^{K}, \ X^K_1 \triangleq \{X_j\}_{j=1}^{K}, \ Y^K_1 \triangleq \{Y_j\}_{j=1}^{K}, \) and all the \( c_i \)'s in this paper are constants which do not depend on \( P \).

For each \( j \), we introduce \( \tilde{X}_j = X_j + \tilde{N}_j \), where \( \tilde{N}_j \) is an i.i.d. sequence of \( \tilde{N}_j \) which is a zero-mean Gaussian random variable with variance \( \sigma^2 < \min(\min_i 1/h^2_{ji}, 1/g^2_i) \). Also, \( \{\tilde{N}_j\}_{j=1}^{K} \) are mutually independent, and are independent of all other random variables. Continuing from
\[ n \sum_{i=1}^{K} R_i \leq h(\tilde{X}_1^K, Y_1^K, Z) - h(\tilde{X}_1^K|Y_1^K, Z) - h(Z) + nc_1 \quad \text{(27)} \]

\[ \leq h(\tilde{X}_1^K, Y_1^K, Z) - h(\tilde{X}_1^K|X_1^K, Y_1^K, Z) - h(Z) + nc_1 \quad \text{(28)} \]

\[ = h(\tilde{X}_1^K, Y_1^K, Z) - h(\tilde{N}_1^K) - h(Z) + nc_1 \quad \text{(29)} \]

\[ \leq h(\tilde{X}_1^K, Y_1^K, Z) - h(Z) + nc_2 \quad \text{(30)} \]

\[ = h(\tilde{X}_1^K) + h(Y_1^K, Z|\tilde{X}_1^K) - h(Z) + nc_2 \quad \text{(31)} \]

\[ \leq h(\tilde{X}_1^K) - h(Z) + nc_3 \quad \text{(32)} \]

where \( \tilde{X}_1^K \triangleq \{ \tilde{X}_j \}_{j=1}^{K} \), and the last inequality is due to the fact that \( h(Y_1^K, Z|\tilde{X}_1^K) \leq nc' \), i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be reconstructed, which is shown as follows

\[
h(Y_1^K, Z|\tilde{X}_1^K) \leq \left[ \sum_{j=1}^{K} h(Y_j|\tilde{X}_1^K) \right] + h(Z|\tilde{X}_1^K) \quad \text{(33)}
\]

\[
= \left[ \sum_{j=1}^{K} h \left( \sum_{i=1}^{K} h_{ij}(\tilde{X}_i - \tilde{N}_i) + N_j | \tilde{X}_1^K \right) \right] + h \left( \sum_{i=1}^{K} g_i(\tilde{X}_i - \tilde{N}_i) + N_Z | \tilde{X}_1^K \right) \quad \text{(34)}
\]

\[
= \left[ \sum_{j=1}^{K} h \left( - \sum_{i=1}^{K} h_{ij} \tilde{N}_i + N_j | \tilde{X}_1^K \right) \right] + h \left( - \sum_{i=1}^{K} g_i \tilde{N}_i + N_Z | \tilde{X}_1^K \right) \quad \text{(35)}
\]

\[
\leq \left[ \sum_{j=1}^{K} h \left( - \sum_{i=1}^{K} h_{ij} \tilde{N}_i + N_j \right) \right] + h \left( - \sum_{i=1}^{K} g_i \tilde{N}_i + N_Z \right) \quad \text{(36)}
\]

\[
\triangleq nc_4 \quad \text{(37)}
\]

Next, we note

\[
h(\tilde{X}_j) \leq h(g_j X_j + N_Z) + nc_5 \leq h(Z) + nc_5, \quad j = 1, \ldots, K \quad \text{(38)}
\]

where the inequalities are due to the differential entropy version of [14] Problem 2.14. In-
Inserting (38) into (32), for any \( j = 1, \ldots, K \), we get

\[
 n \sum_{i=1}^{K} R_i \leq h(\tilde{X}_1^K) - h(Z) + nc_3
\]

\[
 \leq \sum_{i=1}^{K} h(\tilde{X}_i) - h(Z) + nc_3
\]

\[
 \leq \sum_{i=1, i \neq j}^{K} h(\tilde{X}_i) + nc_6
\]

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 \( \tilde{X}_i \) with \( k = i + 1 \) (for \( i = K \), \( k = 1 \)), in (41) as

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

\[
 \leq [h(Y_2) - nR_2] + [h(Y_3) - nR_3] + \cdots + [h(Y_j) - nR_j]
\]

\[
 + [h(Y_{j+2}) - nR_{j+2}] + \cdots + [h(Y_K) - nR_K] + [h(Y_1) - nR_1] + nc_8
\]

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

\[
 2n \sum_{i=1}^{K} R_i \leq (K-1) \left( \frac{n}{2} \log P \right) + nR_{(j+1) \mod K} + nc_9
\]

for \( j = 1, \ldots, K \). Therefore, we have a total of \( K \) bounds in (44) for \( j = 1, \ldots, K \). Summing these \( K \) bounds, we obtain:

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

which gives

\[
 D_{s, \Sigma} \leq \frac{K(K-1)}{2K-1}
\]

completing the converse for IC-EE.

5 Converse for IC-CM

In this section, we develop a converse for the \( K \)-user IC-CM (see Figure 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 $j$:

$$
n \sum_{i=1,i\neq j}^{K} R_i = \sum_{i=1,i\neq j}^{K} H(W_i) = H(W_{-j}^K) \ (47)
$$

$$
\leq I(W_{-j}^K; Y_{-j}^K) - I(W_{-j}^K; Y_j) + nc_1 \ (48)
$$

$$
\leq I(W_{-j}^K; Y_{-j}^K, Y_j) - I(W_{-j}^K; Y_j) + nc_1 \ (49)
$$

$$
= I(W_{-j}^K; Y_{-j}^K | Y_j) + nc_1 \ (50)
$$

$$
\leq I(X_{-j}^K; Y_{-j}^K | Y_j) + nc_1 \ (51)
$$

$$
= h(Y_{-j}^K | Y_j) - h(Y_{-j}^K | Y_j, X_{-j}^K) + nc_1 \ (52)
$$

$$
\leq h(Y_{-j}^K | Y_j) - h(Y_{-j}^K | Y_j, X_1^K) + nc_1 \ (53)
$$

$$
= h(Y_{-j}^K | Y_j) - h(N_{-j}^K | Y_j, X_1^K) + nc_1 \ (54)
$$

$$
\leq h(Y_{-j}^K | Y_j) + nc_12 \ (55)
$$

$$
= h(Y_{-j}^K, Y_j) - h(Y_j) + nc_12 \ (56)
$$

$$
= h(Y^K_1) - h(Y_j) + nc_12 \ (57)
$$

where $W_{-j}^K \triangleq \{W_i\}_{i=1,i\neq j}^{K}$ is the message set containing all unintended messages with respect to receiver $j$, $X_{-j}^K \triangleq \{X_i\}_{i=1,i\neq j}^{K}$ and $Y_{-j}^K \triangleq \{Y_i\}_{i=1,i\neq j}^{K}$.

For each $j$, we introduce $\tilde{X}_j = X_j + \tilde{N}_j$, where $\tilde{N}_j$ is an i.i.d. sequence of $\tilde{N}_j$ which is a zero-mean Gaussian random variable with variance $\sigma_j^2 < \min_j 1/h_{ji}^2$. Also, $\{\tilde{N}_j\}_{j=1}^{K}$ are mutually independent, and are independent of all other random variables. Continuing from (57),

$$
n \sum_{i=1,i\neq j}^{K} R_i \leq h(\tilde{X}_1^K, Y_1^K) - h(\tilde{X}_1^K | Y_1^K) - h(Y_j) + nc_{12} \ (58)
$$

$$
\leq h(\tilde{X}_1^K, Y_1^K) - h(\tilde{X}_1^K | Y_1^K, X_1^K) - h(Y_j) + nc_{12} \ (59)
$$

$$
= h(\tilde{X}_1^K, Y_1^K) - h(\tilde{N}_1^K) - h(Y_j) + nc_{12} \ (60)
$$

$$
\leq h(\tilde{X}_1^K, Y_1^K) - h(Y_j) + nc_{13} \ (61)
$$

$$
= h(\tilde{X}_1^K) + h(Y_1^K | \tilde{X}_1^K) - h(Y_j) + nc_{13} \ (62)
$$

$$
\leq h(\tilde{X}_1^K) - h(Y_j) + nc_{14} \ (63)
$$

where the last inequality is due to the fact that $h(Y_1^K | \tilde{X}_1^K) \leq nc'$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be reconstructed, which
is shown as follows

\[ h(Y^K_i | \tilde{X}^K_i) \leq \sum_{j=1}^{K} h(Y_j | \tilde{X}^K_1) \]  

(64)

\[ = \sum_{j=1}^{K} h \left( \sum_{i=1}^{K} h_{ij}(\tilde{X}_i - \tilde{N}_i) + N_j | \tilde{X}^K_1 \right) \]  

(65)

\[ = \sum_{j=1}^{K} h \left( - \sum_{i=1}^{K} h_{ij} \tilde{N}_i + N_j | \tilde{X}^K_1 \right) \]  

(66)

\[ \leq \sum_{j=1}^{K} h \left( - \sum_{i=1}^{K} h_{ij} \tilde{N}_i + N_j \right) \]  

(67)

\[ \triangleq nc_{15} \]  

(68)

We apply the role of a helper lemma, Lemma 1, to each \( \tilde{X}_i \) with \( k = i + 1 \) (for \( i = K, k = 1 \)), in (63) as

\[ n \sum_{i=1, i \neq j}^{K} R_i \leq h(\tilde{X}^K_i) - h(Y_j) + nc_{14} \]  

(69)

\[ \leq \sum_{i=1}^{K} h(\tilde{X}_i) - h(Y_j) + nc_{14} \]  

(70)

\[ \leq \sum_{i=1}^{K-1} \left[ h(Y_{i+1}) - nR_{i+1} \right] + \left[ h(Y_1) - nR_1 \right] - h(Y_j) + nc_{16} \]  

(71)

\[ = \sum_{i=1}^{K} \left[ h(Y_i) - nR_i \right] - h(Y_j) + nc_{16} \]  

(72)

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

\[ nR_j + 2n \sum_{i=1, i \neq j}^{K} R_i \leq \sum_{i=1, i \neq j}^{K} h(Y_i) + nc_{16} \]  

(73)

\[ \leq (K - 1) \left( \frac{n}{2} \log P \right) + nc_{17} \]  

(74)

for \( j = 1, \ldots, K \). Therefore, we have a total of \( K \) bounds in (74) for \( j = 1, \ldots, K \). Summing these \( K \) bounds, we obtain:

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

(75)
which gives
\[ D_{s,\Sigma} \leq \frac{K(K - 1)}{2K - 1} \] (76)
completing the converse for IC-CM.

6 Achievability

In this section, we provide achievability for the \( K \)-user IC-CM-EE (see Figure 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
\[ D_{s,\Sigma} \geq \frac{K(K - 1)}{2K - 1} \] (77)
is achievable for the \( K \)-user IC-CM-EE.

6.1 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 [43]. We provide the general achievable scheme for \( K > 2 \) in Section 6.2 via cooperative jamming and asymptotic real alignment, and show that it achieves the sum secure d.o.f. in (77) via a detailed performance analysis in Section 6.3.

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 Figure 10 in [38]). Each of them is uniformly and independently drawn from the discrete constellation \( C(a, Q) \) given in (9). 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 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,
\[ V_{ij}, \quad i, j = 1, \ldots, K, j \neq i \] (78)
\[ U_k, \quad k = 1, \ldots, K \] (79)
which are illustrated in Figure 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 Figure 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 Figure 3. We do these simultaneous alignments using asymptotic real alignment technique proposed in [43] and used in [30, 36].

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 $V_{21} = \{v_{21t} : t = 1, \ldots, |T_1|\}$. 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 dimensions:

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

(80)
where \( m \) is a 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.,

\[
|h_{11}T_1 \cap h_{21}T_1| = m^2(m - 1)^2 \approx m^4 = |T_1|
\]

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 Figure 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.

### 6.2 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:

\[
T_i \triangleq \left\{ h_{iis}^r \left( \prod_{j,k=1,j \neq k}^{K} h_{jk}^{r_{jk}} \right) \left( \prod_{j=1}^{K} g_{js}^{s_j} \right) : r_{jk}, s_j \in \{1, \ldots, m\} \right\}
\]

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

\[
M \triangleq m^{1+K(K-1)+K} = m^{K^2+1}
\]

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

\[
b_i^T = [t_{i1}^T, \ldots, t_{i,i-1}^T, t_{i,i+1}^T, \ldots, t_{iK}^T, t_{(i)}^T]
\]  

Then, transmitter \(i\) generates a vector \(a_i\), 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

\[
a_i^T = [v_{1i}^T, \ldots, v_{i,i-1}^T, v_{i,i+1}^T, \ldots, v_{iK}^T, u_i^T]
\]

where \(v_{ij}\) represents the information symbols in \(V_{ij}\), and \(u_i\) represents the cooperative jamming signal in \(U_i\). Each of these vectors has length \(M\), and therefore, the total length of \(a_i\) is \(KM\). The channel input of transmitter \(i\) is

\[
x_i = a_i^T b_i
\]

Before we investigate the performance of this signalling scheme in Section 6.3, 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 \(v_{jk}\) for all \(j, k\) \((j \neq k)\) and \(u_i\) 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

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

The information symbols coming from transmitter 1 are in vectors \(v_{12}, v_{13}, \ldots, v_{1K}\) which are multiplied by coefficients in \(t_{12}, t_{13}, \ldots, t_{1K}\) 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 \(v_{12}, v_{13}, \ldots, v_{1K}\) are \(h_{11} t_{12}, h_{11} t_{13}, \ldots, h_{11} t_{1K}\), 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 $h_{ij}$ in it (but no $h_{jj}$), these dimensions are separate. These correspond to separate boxes of $V_{12}$ and $V_{13}$ at receiver 1 in Figure 3 for the example case of $K = 3$.

On the other hand, all of the cooperative jamming signals from all of the transmitters $u_1, u_2, \ldots, u_K$ come to receiver 1 with received coefficients $h_{11}t_{(1)}, h_{21}t_{(2)}, \ldots, h_{K1}t_{(K)}$, which are the dimensions in the sets $h_{11}T_1, h_{21}T_2, \ldots, h_{K1}T_K$, respectively. We note that 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 Figure 3 for the example case of $K = 3$.

Next, we note that each $u_i$ is aligned together with all of the $v_{ji}$ coming from the $j$th transmitter, with $j \neq i$ and $j \neq 1$, at receiver 1. Note that $u_i$ occupies dimensions $h_{ii}T_i$ and $v_{ji}$ (for any $j \neq i$ and $j \neq 1$) occupies dimensions $h_{jj}T_i$ at receiver 1. From the arguments in Section 6.1, $u_i$ and $v_{ji}$ (with $j \neq i$ and $j \neq 1$) are asymptotically aligned. More formally, we note that $u_i$ occupies dimensions $h_{ii}T_i$ which is contained in $\tilde{T}_i$. Similarly, all $v_{ji}$, with $j \neq i$ and $j \neq 1$, occupy dimensions $h_{jj}T_i$, respectively, which are all contained in $\tilde{T}_i$. Therefore, $u_i$ and all $v_{ji}$ (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 Figure 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

$$R_1 \triangleq \left( \bigcup_{j=2}^{K} h_{11}T_j \right) \bigcup \left( \bigcup_{j=2}^{K} \tilde{T}_j \right) \bigcup \tilde{T}_1$$

are rationally independent, and thereby the cardinality of $R_1$ is

$$M_R \triangleq |R_1| = (K - 1)m^{1+K(K-1)+K} + K(m + 1)^{1+K(K-1)+K}$$

$$= (K - 1)m^{K^2+1} + K(m + 1)^{K^2+1}$$

### 6.3 Performance Analysis

We will compute the secrecy rates achievable with the asymptotic alignment based scheme proposed in Section 6.2 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

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

18
where for convenience we denote $Z$ by $Y_0$, $V_i^K \triangleq \{V_j\}_{j=1}^K$ and $K_{0,-i} = \{0, 1, \ldots, i-1, i+1, \ldots, K\}$. The auxiliary random variables $\{V_i\}_{i=1}^K$ are mutually independent, and for each $i$, we have the following Markov chain $V_i \rightarrow X_i \rightarrow (Y_1, \ldots, Y_K)$.

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 A.

We apply Theorem 2 to our alignment based scheme proposed in Section 6.2 by selecting $V_i$ used in (91) as

$$V_i \triangleq (v_{i1}^T, \ldots, v_{i,i-1}^T, v_{i,i+1}^T, \ldots, v_{iK}^T)$$

for $i = 1, \ldots, K$. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M_R+\delta)}}$ and $a = \frac{\gamma P^2}{Q}$, based on Lemma 2, the probability of error of estimating $V_i$ based on $Y_i$ can be upper bounded by a function decreasing exponentially fast in $P$, by choosing a $\gamma$, a positive constant independent of $P$ to normalize the average power of the input signals, as

$$0 < \gamma \leq \frac{1}{\sum_{t \in T_i} |t|} = \frac{1}{\sum_{i=1}^K \sum_{t \in T_i} |t_i|}$$

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

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

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

where $o(\cdot)$ is the little-$o$ function. This provides a lower bound for the first term in (91).

Next, we need to derive an upper bound for the second item in (91), 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 $V_i \rightarrow (\sum_{k=1}^K h_{kj} X_k, V_{-i}^K) \rightarrow Y_j$,

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

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

$$\leq I \left( V_i; Y_j \middle| V_{-i}^K \right)$$

$$= \frac{1}{2} \log P$$

Therefore, the secrecy penalty is upper bounded by $\frac{1}{2} \log P$, as desired.
where $V^K_1 = \{V_1, \ldots, V_K\}$. The first term in (97) can be rewritten as

$$H \left( \sum_{k=1}^{K} h_{kj} X_k \bigg| V^K_i \right) = H \left( \sum_{k=1}^{K} h_{kj} u_k^T t_{(k)} + \sum_{k=1}^{K} h_{ij} v_{ik}^T t_{ik} \right) = H \left( h_{ij} u_i^T t_{(i)} + \sum_{k=1}^{K} \left[ h_{ij} v_{ik}^T t_{ik} + h_{kj} u_k^T t_{(k)} \right] \right)$$

(98)

Note that, for a given $k$, the vectors $t_{ik}$ and $t_{(k)}$ represent the same dimensions $T_k$, and $h_{ij}, h_{kj} \in T_k$ for all $k \neq i$, which implies that $h_{ij} T_k, h_{kj} T_k \in \hat{T}_k$. 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.,

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

(100)

Therefore, the first term in (97) can be further upper bounded as

$$H \left( \sum_{k=1}^{K} h_{kj} X_k \bigg| V^K_i \right) = H \left( h_{ij} u_i^T t_{(i)} + \sum_{k=1}^{K} \left[ h_{ij} v_{ik}^T t_{ik} + h_{kj} u_k^T t_{(k)} \right] \right) \leq \log \left[ (2Q + 1)^M (4Q + 1)^{(K-1)M_\delta} (2Q + 1)^{(K-1)(M-M_\delta)} \right]$$

(102)

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

(103)

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

(104)

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

(105)
The second term in (97) is exactly the entropy of \( \{ u_k \}_{k=1}^K \) vectors, i.e.,

\[
H \left( \sum_{k=1}^K h_{kj} X_k | V_i^K \right) = H \left( \sum_{k=1}^K h_{kj} u_k^T t(k) \right) 
= \log(2Q + 1)^{KM} 
\]  \hspace{1cm} (106)

\[
= \frac{K m K^2 + (1 - \delta)}{(K - 1)m K^2 + K (m + 1) K^2 + \delta \left( \frac{1}{2} \log P \right) + o(\log P)} 
\]  \hspace{1cm} (107)

Substituting (105) and (109) into (97), we get

\[
I(V_i; Y_j | V_i^K) \leq H \left( \sum_{k=1}^K h_{kj} X_k | V_i^K \right) - H \left( \sum_{k=1}^K h_{kj} X_k | V_1^K \right) 
\leq \frac{1 + (K - 1) \left( 1 - \frac{1}{m} \right)^2 + 2(K - 1) \left[ 1 - \left( 1 - \frac{1}{m} \right)^2 \right] - K}{K - 1 + K \left( 1 + \frac{1}{m} \right) K^2 + \frac{\delta}{m K^2 + 1} \left( \frac{1}{2} \log P \right) + o(\log P)} 
\]  \hspace{1cm} (110)

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 \( i \in K \) and \( j = 0 \), i.e., \( Y_0 = Z \) the external eavesdropper, we should derive a new upper bound for the second term in (97), i.e., \( I(V_i; Z | V_i^K) \). By similar steps, we have

\[
I(V_i; Z | V_i^K) \leq I \left( V_i; \sum_{k=1}^K g_k X_k | V_i^K \right) 
\leq H \left( \sum_{k=1}^K g_k X_k | V_i^K \right) - H \left( \sum_{k=1}^K g_k X_k | V_1^K \right) 
\leq H \left( \sum_{k=1}^K g_k X_k | V_i^K \right) - \log(2Q + 1)^{KM} 
\]  \hspace{1cm} (113)}
Here, we need to upper bound the first item in (116). We first observe that

\[
H \left( \sum_{k=1}^{K} g_k X_k \big| V^K_{-i} \right) = H \left( \sum_{k=1}^{K} g_k^T t_{(k)} + \sum_{k=1, k \neq i}^{K} g_i^T t_{ik} \right)
\]

\[
= H \left( g_i^T t_{(i)} + \sum_{k=1, k \neq i}^{K} \left[ g_k^T t_{(k)} + g_i^T t_{ik} \right] \right) \tag{117}
\]

Firstly, note that, \(t_{(k)}\) and \(t_{ik}\) represent the same set \(T_k\). Therefore, for different \(k\), the dimensions are distinguishable. Secondly, due to reasons similar to (100), we conclude that

\[
H \left( \sum_{k=1}^{K} g_k X_k \big| V^K_{-i} \right) = H \left( g_i^T t_{(i)} + \sum_{k=1, k \neq i}^{K} \left[ g_k^T t_{(k)} + g_i^T t_{ik} \right] \right) \tag{119}
\]

\[
\leq \log \left[ \left(2Q + 1\right)^M \left(4Q + 1\right)^{(K-1)M_\delta} \left(2Q + 1\right)^{2(K-1)(M - M_\delta)} \right] \tag{120}
\]

\[
\leq \log \left[ Q^{M + (K-1)M_\delta + 2(K-1)(M - M_\delta)} \right] + o(\log P) \tag{121}
\]

\[
\leq \frac{[M + (K-1)M_\delta + 2(K-1)(M - M_\delta)](1 - \delta)}{(K - 1)m^{K^2 + 1} + K(m + 1)^{K^2 + 1} + \delta} \left( \frac{1}{2} \log P \right) + o(\log P) \tag{122}
\]

Substituting (122) into (116), we attain an upper bound which is the same as the upper bound for \(I(V_i; Y_j|V^K_{-i})\), i.e.,

\[
I(V_i; Z|V^K_{-i}) \leq \frac{K \frac{2m - 1}{m^2} (1 - \delta)}{K - 1 + K \left(1 + \frac{1}{m}\right)^{K^2 + 1} + \frac{\delta}{m^{K^2 + 1}}} \left( \frac{1}{2} \log P \right) + o(\log P) \tag{123}
\]

Substituting (95), (112), and (123) into (91), we obtain a lower bound for the achievable secrecy rate \(R_i\) as

\[
R_i \geq \frac{[(K - 1) - K \frac{2m - 1}{m^2}]}{K - 1 + K \left(1 + \frac{1}{m}\right)^{K^2 + 1} + \frac{\delta}{m^{K^2 + 1}}} \left( \frac{1}{2} \log P \right) + o(\log P) \tag{124}
\]

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 (77).
7 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.

A Proof of Theorem 2

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 (91) on $V_{K-1}^i$. 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

$$I(V_i; Y_j | V_{K-1}^i) = I(V_i; Y_j, V_{K}^i) = I(V_i; \tilde{Y}_j)$$

(125)

where $\tilde{Y}_j = (Y_j, V_{K}^i)$ 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 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

$$I(V_i; Y_{(i)} | V_{K-1}^i) = \max_{j \in K, j \neq i} I(V_i; Y_j | V_{K-1}^i)$$

(126)

That is, $Y_{(i)}$ is the strongest eavesdropper with respect to transmitter $i$. The achievable rate in (91) 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

$$H(W_i | Y^{(i)}, V^K_{-i}) \geq H(W_i) - n\epsilon^{(i)}, \quad i = 1, \ldots, K$$ (127)

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 (127) fit the created equivalent view of the channel better. As we show next, secrecy constraints in (127) imply our original secrecy constraints in (4) and (5).

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

$$H(W_i | Y_j, V^K_{-i}) \geq H(W_i | Y^{(i)}, V^K_{-i}) \geq H(W_i) - n\epsilon^{(i)}$$ (128)

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 (127) for all $i$ implies the original secrecy constraints in (4) and (5) follows from the following derivation:

$$H(W^K_{-j} | Y_j) \geq H(W^K_{-j} | Y_j, W_j)$$ (129)
$$\geq \sum_{i \neq j} H(W_i | Y_j, W^K_{-i})$$ (130)
$$\geq \sum_{i \neq j} H(W_i | Y_j, V^K_{-i}, W^K_{-i})$$ (131)
$$= \sum_{i \neq j} H(W_i | Y_j, V^K_{-i})$$ (132)
$$\geq \sum_{i \neq j} H(W_i | Y^{(i)}, V^K_{-i})$$ (133)
$$\geq \sum_{i \neq j} \left[ H(W_i) - n\epsilon^{(i)} \right]$$ (134)
$$= H(W^K_{-j}) - n\epsilon^{(-j)}$$ (135)
where (132) is due to the Markov chain $W^K_i \rightarrow (Y_j, V^K_{-i}) \rightarrow W_i$. Similarly,

$$H(W^K|Z) \geq \sum_i H(W_i|Z, W^K_i)$$ (136)

$$\geq \sum_i H(W_i|Z, V^K_{-i}, W^K_i)$$ (137)

$$= \sum_i H(W_i|Z, V^K_i)$$ (138)

$$\geq \sum_i H(W_i|Y^{(i)}, V^K_i)$$ (139)

$$\geq \sum_i \left[ H(W_i) - n\epsilon^{(i)} \right]$$ (140)

$$= H(W^K) - n\epsilon^{(Z)}$$ (141)

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

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

$$R_i = I(V_i; Y_i) - I(V_i; Y^{(i)}|V^K_{-i}) - \epsilon$$ (142)

$$R^c_i = I(V_i; Y^{(i)}|V^K_{-i}) - \epsilon$$ (143)

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

$$p(v_i) = \prod_{t=1}^{n} p(v_{it})$$ (144)

and constructs a codebook as

$$C_i \triangleq \left\{ v_i(w_i, w^c_i) : w_i \in \{1, \ldots, 2^{nR_i}\}, w^c_i \in \{1, \ldots, 2^{nR^c_i}\} \right\}$$ (145)

To transmit a message $w_i$, transmitter $i$ chooses an element $v_i$ from the sub-codebook $C_i(w_i)$

$$C_i(w_i) \triangleq \left\{ v_i(w_i, w^c_i) : w^c_i \in \{1, \ldots, 2^{nR^c_i}\} \right\}$$ (146)

and generates a channel input sequence based on

$$p(x_i|v_i)$$ (147)

Due to the code construction, we have $R_i + R^c_i < I(V_i; Y_i)$, 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 $\max_i Pr(e_i^{(n_i)}) \leq \epsilon$. 

25
For the equivocation calculation, we consider the following conditional entropy as discussed before:

\[
H(W_i|Y^{(i)}, V_{-i}^K) = H(W_i, Y^{(i)}|V_{-i}^K) - H(Y^{(i)}|V_{-i}^K) \\
= H(W_i, V_i, Y^{(i)}|V_{-i}^K) - H(V_i|W_i, Y^{(i)}, V_{-i}^K) - H(Y^{(i)}|V_{-i}^K) \\
= H(W_i, V_i|V_{-i}^K) + H(Y^{(i)}|W_i, V_i, V_{-i}^K) - H(V_i|W_i, Y^{(i)}, V_{-i}^K) \\
- H(Y^{(i)}|V_{-i}^K) \\
= H(W_i, V_i|V_{-i}^K) - H(V_i|W_i, Y^{(i)}, V_{-i}^K) + H(Y^{(i)}|V_i, V_{-i}^K) - H(Y^{(i)}|V_{-i}^K) \\
\tag{151}
\]

where the last equality is due to the Markov chain \( W_i \to (V_i, V_{-i}^K) \to Y^{(i)} \).

The first term in (151) is exactly the entropy of codebook \( C_i \)

\[
H(V_i) = n(R_i + R_i^c) \\
\tag{152}
\]

To bound the second term in (151), we have the following observation: Given the message \( W_i = w_i \) and the received sequences \( Y^{(i)} = y^{(i)} \) and genie-aided sequences \( V_{-i}^K = v_{-i}^K \), receiver \( Y^{(i)} \) can decode the codeword \( v_i(w_i, w_i^c) \) with arbitrarily small probability of error \( \lambda(w_i)^{(n)} \) as \( n \) gets very large. More formally: by giving \( W_i = w_i, V_{-i}^K = v_{-i}^K \), receiver \( Y^{(i)} \) decodes \( V_i \) if there is a unique \( w_i^c \) such that

\[
(v_i(w_i, w_i^c), y^{(i)}) \in T_e^{(n)}(P_{V_i,Y^{(i)}|V_{-i}^K}) \\
\tag{153}
\]

Otherwise, the receiver declares an error. Without loss of generality, we assume that \( v_i(w_i, w_i^c) \) is sent and denote the event \( \{ (v_i(w_i, w_i^c), y^{(i)}) \in T_e^{(n)}(P_{V_i,Y^{(i)}|V_{-i}^K}) \} \) as \( E_j \). Therefore, the probability of error \( \lambda(w_i)^{(n)} \) can be bounded as

\[
\lambda(w_i)^{(n)} \leq \Pr(E_i^c) + \sum_{j \neq 1} \Pr(E_j) \\
\tag{154}
\]

where the probability here is conditioned on the event that \( v_i(w_i, w_i^c) \) is sent. By joint typicality, we know that \( \Pr(E_i^c) \leq \epsilon_1 \) for sufficiently large \( n \), and

\[
\Pr(E_j) \leq 2^{nH(V_i,Y^{(i)}|V_{-i}^K) - nH(V_i) - nH(Y^{(i)}|V_{-i}^K) - n\epsilon_2} = 2^{-nI(V_i;Y^{(i)}|V_{-i}^K) - n\epsilon_2} \\
\tag{155}
\]

Hence,

\[
\lambda(w_i)^{(n)} \leq \epsilon_1 + 2^{nR_i^c} 2^{-nI(V_i;Y^{(i)}|V_{-i}^K) - n\epsilon_2} \\
\tag{156}
\]

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 by Fano's inequality further implies that

$$H(V_i | W_i, Y^{(i)}, V^K_{-i}) = \sum_{W_i = w_i, Y^{(i)} = y^{(i)}, V^K_{-i} = v^K_{-i}} H(V_i | W_i, Y^{(i)}, V^K_{-i}) \leq n \epsilon_4 \quad (157)$$

The third term in (151) can be lower bounded as follows:

$$H(Y^{(i)} | V_i, V^K_{-i}) = \sum_{v_i, v^K_{-i}} \Pr(V_i = v_i) \Pr(V^K_{-i} = v^K_{-i}) H(Y^{(i)} | V_i = v_i, V^K_{-i} = v^K_{-i}) \quad (158)$$

$$\geq \sum_{(v_i, v^K_{-i}) \in T^{(i)}(P_{V_i, v^K_{-i}})} \left[ \Pr(V_i = v_i) \Pr(V^K_{-i} = v^K_{-i}) H(Y^{(i)} | V_i = v_i, V^K_{-i} = v^K_{-i}) \right] \quad (159)$$

$$\geq \sum_{(v_i, v^K_{-i}) \in T^{(i)}(P_{V_i, v^K_{-i}})} \left[ \Pr(V_i = v_i) \Pr(V^K_{-i} = v^K_{-i}) \sum_{(a, b) \in V_i \times V^K_{-i}} N(a, b | v_i, v^K_{-i}) \sum_{y^{(i)} \in Y^{(i)}} -p(y^{(i)} | a, b) \log p(y^{(i)} | a, b) \right] \quad (160)$$

$$\geq \sum_{(v_i, v^K_{-i}) \in T^{(i)}(P_{V_i, v^K_{-i}})} \left[ \Pr(V_i = v_i) \Pr(V^K_{-i} = v^K_{-i}) \sum_{(a, b) \in V_i \times V^K_{-i}} n \left( \Pr(V_i = a, V^K_{-i} = b) - \epsilon_5 \right) \right. \left. \sum_{y^{(i)} \in Y^{(i)}} -p(y^{(i)} | a, b) \log p(y^{(i)} | a, b) \right] \quad (161)$$

$$\geq \sum_{(v_i, v^K_{-i}) \in T^{(i)}(P_{V_i, v^K_{-i}})} \left[ n \left( \Pr(V_i = v_i) \Pr(V^K_{-i} = v^K_{-i}) H(Y^{(i)} | V_i, V^K_{-i}) - \epsilon_6 \right) \right] \quad (162)$$

$$\geq (1 - \epsilon_7) n H(Y^{(i)} | V_i, V^K_{-i}) - n \epsilon_8 \quad (163)$$

$$\geq n H(Y^{(i)} | V_i, V^K_{-i}) - n \epsilon_9 \quad (164)$$

To compute the forth term in (151), we define

$$\hat{Y}^{(i)} = \begin{cases} Y^{(i)}, & \text{if } (v^K_{-i}, y^{(i)}) \in T^{(i)}(P_{Y^{(i)}}, Y^{(i)}) \\ \text{arbitrary}, & \text{otherwise} \end{cases} \quad (165)$$
Then, we obtain

\[ H(Y^{(i)}|V_{-i}^K) = \sum_{v_{-i}^K} \Pr(V_{-i}^K = v_{-i}^K)H(Y^{(i)}|V_{-i}^K = v_{-i}^K) \]  

(166)

\[ \leq \sum_{v_{-i}^K} \Pr(V_{-i}^K = v_{-i}^K)H(Y^{(i)}, \hat{Y}^{(i)}|V_{-i}^K = v_{-i}^K) \]  

(167)

\[ = \sum_{v_{-i}^K} \Pr(V_{-i}^K = v_{-i}^K)\left[H(Y^{(i)}|V_{-i}^K = v_{-i}^K) + H(Y^{(i)}|V_{-i}^K = v_{-i}^K, \hat{Y}^{(i)})\right] \]  

(168)

\[ \leq nH(Y^{(i)}|V_{-i}^K) + n\epsilon_{10} + \sum_{v_{-i}^K} \Pr(V_{-i}^K = v_{-i}^K)H(Y^{(i)}|V_{-i}^K = v_{-i}^K, \hat{Y}^{(i)}) \]  

(169)

Combining Fano’s inequality and the fact that

\[ \Pr(Y^{(i)} \neq \hat{Y}^{(i)}) \leq \Pr\left\{(V_{-i}^K, Y^{(i)}) \notin T^{(n)}(P_{V_{-i}^K,Y^{(i)}})\right\} \]  

(170)

is arbitrarily small for sufficiently large \( n \), (169) implies

\[ H(Y^{(i)}|V_{-i}^K) \leq nH(Y^{(i)}|V_{-i}^K) + n\epsilon_{10} + n\epsilon_{11} \]  

(171)

Substituting (152), (157), (164), and (171) into (151), we conclude that

\[ H(W_i|Y^{(i)}, V_{-i}^K) \geq H(W_i) - n\epsilon^{(i)} \]  

(172)

where \( \epsilon^{(i)} \) is small for sufficiently large \( n \), which completes the proof.

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 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] J. Xu, Y. Cao, and B. Chen. Capacity bounds for broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 55(10):4529–4542, October 2009.
[7] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, June 2008.

[8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. Secure broadcasting: The secrecy rate region. In *46th Annual Allerton Conference on Communications, Control and Computing*, Monticello, IL, September 2008.

[9] E. Ekrem and S. Ulukus. On secure broadcasting. In *42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, October 2008.

[10] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, March 2009.

[11] E. Ekrem and S. Ulukus. Secure broadcasting using multiple antennas. *Journal of Communications and Networks*, 12(5):411–432, October 2010.

[12] X. He and A. Yener. A new outer bound for the Gaussian interference channel with confidential messages. In *43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2009.

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

[14] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, December 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*, 54(6):2735–2751, June 2008.

[16] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[17] Y. Liang and H. V. Poor. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, March 2008.

[18] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[19] X. Tang, R. Liu, P. Spasojevic, and H.V. Poor. The Gaussian wiretap channel with a helping interferer. In *IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008.
[20] Y. Oohama. Relay channels with confidential messages. *IEEE Trans. Inf. Theory, Special issue on Information Theoretic Security*, submitted Nov 2006. Also available at [arXiv/cs/0611125v7](http://arxiv.org/abs/cs/0611125v7).

[21] L. Lai and H. El Gamal. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, September 2008.

[22] M. Yuksel and E. Erkip. The relay channel with a wiretapper. In *41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[23] M. Bloch and A. Thangaraj. Confidential messages to a cooperative relay. In *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[24] X. He and A. Yener. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory*, 56(8):3807–3827, August 2010.

[25] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 57(1):137–155, January 2011.

[26] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Compound wiretap channels. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, March 2009.

[27] E. Ekrem and S. Ulukus. Degraded compound multi-receiver wiretap channels. *IEEE Trans. Inf. Theory*, 58(9):5681–5698, September 2012.

[28] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. In *IEEE Information Theory Workshop on Networking and Information Theory*, Volos, Greece, June 2009.

[29] 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.

[30] J. Xie and S. Ulukus. Real interference alignment for the K-user Gaussian interference compound wiretap channel. In *48th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2010.

[31] X. He and A. Yener. Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels. *IEEE Trans. Inf. Theory*, submitted July 2009. Also available at [arXiv:0907.5388](http://arxiv.org/abs/0907.5388).

[32] X. He. *Cooperation and information theoretic security in wireless networks*. Ph.D. dissertation, Pennsylvania State University, Pennsylvania, 2010.
[33] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees-of-freedom of the multiple-access-channel. *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729](http://arxiv.org/abs/1003.0729).

[34] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. Inf. Theory*, 58(3):1594–1611, March 2012.

[35] T. Gou and S. A. Jafar. On the secure degrees of freedom of wireless X networks. In *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

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

[37] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2012.

[38] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. Submitted to *IEEE Trans. on Information Theory*, September 2012. Also available at [arXiv:1209.5370](http://arxiv.org/abs/1209.5370).

[39] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming. In *Conference on Information Sciences and Systems*, 2013.

[40] J. Xie and S. Ulukus. Sum secure degrees of freedom of two unicast layered wireless networks. *IEEE Journal on Selected Areas in Communications - Signal Processing Techniques for Wireless Physical Layer Security*, to appear.

[41] 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.

[42] 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](http://arxiv.org/abs/0908.1208).

[43] 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](http://arxiv.org/abs/0908.2282).

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