Secure Degrees of Freedom of One-hop Wireless Networks*

Jianwei Xie Sennur Ulukus

Department of Electrical and Computer Engineering

University of Maryland, College Park, MD 20742

xiejw@umd.edu *ulukus@umd.edu*

September 22, 2012

Abstract

We study the secure degrees of freedom (d.o.f.) of one-hop wireless networks by considering four fundamental wireless network structures: Gaussian wiretap channel, Gaussian broadcast channel with confidential messages, Gaussian interference channel with confidential messages, and Gaussian multiple access wiretap channel. The secrecy capacity of the canonical Gaussian wiretap channel does not scale with the transmit power, and hence, the secure d.o.f. of the Gaussian wiretap channel with no helpers is zero. It has been known that a strictly positive secure d.o.f. can be obtained in the Gaussian wiretap channel by using a helper which sends structured cooperative signals. We show that the exact secure d.o.f. of the Gaussian wiretap channel with a helper is $\frac{1}{2}$. Our achievable scheme is based on real interference alignment and cooperative jamming, which renders the message signal and the cooperative jamming signal *separable* at the legitimate receiver, but *aligns* them perfectly at the eavesdropper preventing any reliable decoding of the message signal. Our converse is based on two key lemmas. The first lemma quantifies the *secrecy penalty* by showing that the net effect of an eavesdropper on the system is that it eliminates one of the independent channel inputs. The second lemma quantifies the *role of a helper* by developing a direct relationship between the cooperative jamming signal of a helper and the message rate. We extend this result to the case of M helpers, and show that the exact secure d.o.f. in this case is $\frac{M}{M+1}$. We then generalize this approach to more general network structures with *multiple messages.* We show that the sum secure d.o.f. of the Gaussian broadcast channel with confidential messages and M helpers is 1, the sum secure d.o.f. of the two-user interference channel with confidential messages is $\frac{2}{3}$, the sum secure d.o.f. of the two-user interference channel with confidential messages and M helpers is 1, and the sum secure d.o.f. of the K-user multiple access wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$.

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

1 Introduction

We study secure communications in one-hop wireless networks from an information-theoretic point of view. Wyner introduced the wiretap channel [1], in which a legitimate transmitter wishes to send a message to a legitimate receiver secret from the eavesdropper. The capacity-equivocation region was originally found for the degraded wiretap channel by Wyner [1], then generalized to the general wiretap channel by Csiszar and Korner [2], and extended to the Gaussian wiretap channel by Leung-Yan-Cheong and Hellman [3]. Multi-user versions of the wiretap channel have been studied recently, e.g., broadcast channels with confidential messages [4,5], multi-receiver wiretap channels [6–8] (see also a survey on extensions of these to MIMO channels [9]), two-user interference channels with confidential messages [4, 10], multiple access wiretap channels [11–15], relay eavesdropper channels [16–21], compound wiretap channels [22, 23]. Since in most multi-user scenarios it is difficult to obtain the exact secrecy capacity region, achievable secure degrees of freedom (d.o.f.) at high signal-to-noise ratio (SNR) cases have been studied for several channel structures, such as the K-user Gaussian interference channel with confidential messages [24, 25], the K-user interference channel with external eavesdroppers [26], the Gaussian wiretap channel with one helper [27,28], the Gaussian multiple access wiretap channel [29,30], and the wireless X network [31].

In the Gaussian wiretap channel, the secrecy capacity is the difference between the channel capacities of the transmitter-receiver and the transmitter-eavesdropper pairs. 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 multi-user scenarios. In a multi-user network, focusing on a specific transmitter-receiver pair, other (independent) transmitters can be understood as helpers which can improve the individual secrecy rate of this specific pair by cooperatively jamming the eavesdropper [11, 12, 15, 32].[1] These cooperative jamming signals also limit the decoding performance of the legitimate receiver. It is also known that if the helper nodes transmit independent identically distributed (i.i.d.) Gaussian cooperative jamming signals in a Gaussian wiretap channel, then the secure d.o.f. is still zero [11, 12, 30, 32]. Such i.i.d. Gaussian signals, while maximally jam the eavesdropper, also maximally hurt the legitimate user's decoding capability. Therefore, we expect that strictly positive secure d.o.f. may be achieved with some *weak* jamming signals. Confirming this intuition, [27, 28] achieved positive secure d.o.f. by using nested lattice codes in a Gaussian wiretap channel with a helper. In this paper, we obtain the exact secure d.o.f. of several Gaussian network structures, including the Gaussian wiretap channel with a helper, by characterizing this trade-off in the cooperative jamming signals of the helpers.

[1]Note that, if reliability was the only concern, then in order to maximize the reliable rate of a given transmitter-receiver pair, all other independent transmitters must remain silent. However, when secrecy in addition to reliability is a concern, then independent helpers can improve the secrecy rate of a given transmitter-receiver pair by transmitting signals [11, 12, 15, 32].

We start by considering the Gaussian wiretap channel with a single helper, as shown in Figure 1. In this channel model, secure d.o.f. with i.i.d. Gaussian cooperative signals is zero [32], and strictly positive secure d.o.f. can be obtained, for instance, by using nested lattice codes [27, 28]. Considering this model as a special case of other channel models, we can verify that $\frac{1}{4}$ secure d.o.f. can be achieved as a symmetric individual rate on the two-user interference channel with external eavesdroppers [26] and on the multiple access wiretap channel [29]. References [33] and [28, Theorem 5.4 on page 126] showed that with integer lattice codes a secure d.o.f. of $\frac{1}{2}$ can be achieved if the channel gains are *irrational algebraic numbers.* While such class of channel gains has zero Lebesgue measure, the idea behind this achievable scheme can be generalized to much larger set of channel gains. The enabling idea behind this achievable scheme is as follows: If the cooperative jamming signal from the helper and the message signal from the legitimate user can be aligned in the same *dimension* at the eavesdropper, then the secrecy penalty due to the information leakage to the eavesdropper can be upper bounded by a constant, while the information transmission rate to the legitimate user can be made to scale with the transmit power. Following this insight, we propose an achievable scheme based on real interference alignment [34, 35] and cooperative jamming to achieve $\frac{1}{2}$ secure d.o.f. for *almost all channel gains.* This constitutes the best known achievable secure d.o.f. for the Gaussian wiretap channel with a helper. The cooperative jamming signal from the helper can be distinguished from the message signal at the legitimate receiver by properly designing the structure of the signals from both transmitters; meanwhile, they can be aligned together at the observation space of the eavesdropper to ensure undecodability of the message signal, hence secrecy (see Figure 7). Intuitively, the end result of $\frac{1}{2}$ secure d.o.f. comes from the facts that the cooperative jamming signal and the message signal should be of about the same size to align at the eavesdropper, and they should be separable at the legitimate receiver, who can decode at most a total of 1 d.o.f. We analyze the rate and equivocation achieved by this scheme by using the Khintchine-Groshev theorem of Diophantine approximation in number theory.

For the converse for this channel model, the best known upper bound is $\frac{2}{3}$ [28, Theorem 5.3 on page 126] which was obtained by adding virtual nodes to the system and using the upper bound developed in [36]. Reference [36] developed upper bounds for the secure d.o.f. of the multiple-antenna compound wiretap channel by exploring the correlation between the n-letter observations of a group of legitimate receivers and a group of eavesdroppers, instead of working with single-letter expressions. Our converse works with n-letter observations as well. Our converse has two key steps. First, we upper bound the secrecy rate by the difference of the sum of differential entropies of the channel inputs of the legitimate receiver and the helper and the differential entropy of the eavesdropper's observation. This shows that, the secrecy penalty due to the eavesdropper's observation is tantamount to eliminating one of the independent channel inputs. As a result, the final upper bound involves only the differential entropy of the channel input of the independent helper. In the second step, we

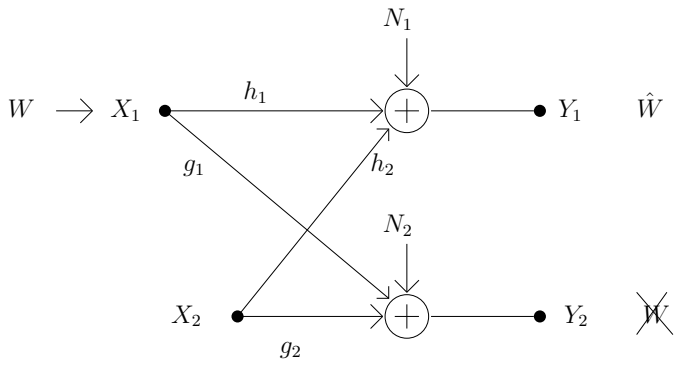

Figure 1: Gaussian wiretap channel with one helper.

develop a relationship between the cooperative jamming signal from the independent helper and the message rate. The goal of the cooperative jamming signal is to further confuse the eavesdropper. However, the cooperative jamming signal appears in the channel output of the legitimate user also. Intuitively, if the legitimate user is to reliably decode the message signal which is mixed with the cooperative jamming signal, there must exist a constraint on the cooperative jamming signal. Our second step identifies this constraint by developing an upper bound on the differential entropy of the cooperative jamming signal in terms of the message rate. These two steps give us an upper bound of $\frac{1}{2}$ secure d.o.f. for the Gaussian wiretap channel with a helper, which matches our achievable lower bound. This concludes that the exact secure d.o.f. of the Gaussian wiretap channel with a helper is $\frac{1}{2}$ for *almost all channel gains*.

We then generalize our result to the case of M independent helpers. We show that the exact secure d.o.f. in this case is $\frac{M}{M+1}$. Our achievability extends our original achievability for the one-helper case in the following manner: The transmitter sends its message by employing M independent sub-messages, and the M helpers send independent cooperative jamming signals. Each cooperative jamming signal is aligned with one of the M sub-messages at the eavesdropper to ensure secrecy (see Figure 8). Therefore, each sub-message is protected by one of the M helpers. Our converse is an extension of the converse in the one-helper case. In particular, we upper bound the secrecy rate by the difference of the sum of the differential entropies of all of the channel inputs and the differential entropy of the eavesdropper's observation. The secrecy penalty due to the eavesdropper's observation eliminates one of the channel inputs, which we choose as the legitimate user's channel input. We then utilize the relationship we developed between the differential entropy of each of the cooperative jamming signals and the message rate. The upper bound so developed matches the achievability lower bound, giving the exact secure d.o.f. for the M-helper case.

As an important extension of the single-message one-helper problem, we consider the broadcast channel with confidential messages and one-helper, where a transmitter wishes to send two messages securely to two users on a broadcast channel while keeping each message secure from the unintended receiver. Without a helper, the sum secure d.o.f. of this channel

model is zero. We show that with one helper, the exact sum secure d.o.f. is 1. The sum secure d.o.f. remains the same as more helpers are added. The achievability for the one-helper case is as follows: The transmitter sends the channel input by putting two messages on different *rational dimensions*. Meanwhile, the cooperative jamming signal from the helper is designed in such a way that it aligns with the unintended message, but leaves the intended message intact, at each receiver (see Figure 9). The converse for this case follows from the converse without any secrecy constraints for the Gaussian broadcast channel, which is 1.

Cooperative jamming based achievable schemes are intuitive for the independent-helper problems due to the fact that the helpers do not have messages of their own. Such schemes can be extended to multiple-transmitter (with independent messages) settings, such as, interference channels with confidential messages and multiple access wiretap channel, etc. All previous works extended this approach in the following way: Each transmitter simply sends one message signal, and the message signals from all of the transmitters are *aligned* together at the eavesdropper. Due to the mixture of the message signals, the eavesdropper is confused regarding any one of the message signals, and a positive secure d.o.f. is achievable. However, this approach is sub-optimal. To achieve optimal secure d.o.f., we need to design the structure of the channel inputs more carefully. We propose the following transmission structure: Besides the message carrying signal, each transmitter also sends a cooperative jamming signal. The exact number and the structure of the message signals and the cooperative jamming signals depend on the specific network structure.

For the two-user Gaussian interference channel with confidential messages, previously known lower bounds for the sum secure d.o.f. are $\frac{1}{3}$ [31] and 0 [24], which come from the general results for the K-user case: $\frac{K-1}{2K-1}$ [31] and $\frac{K-2}{2K-2}$ [24]. The individual secure d.o.f. of $\frac{1}{2}$ achieved in [33] and [28, Theorem 5.4 on page 126] in the context of the wiretap channel with a helper (for the class of algebraic irrational channel gains) can also be understood as a lower bound for the sum secure d.o.f. for the two-user interference channel with confidential messages. We show that, by using interference alignment and cooperative jamming at both transmitters, we can achieve a sum secure d.o.f. of $\frac{2}{3}$ for *almost all channel gains*, which is better than all previously known achievable secure d.o.f. We design an achievable scheme in which each transmitter sends a mixed signal containing the message signal and a cooperative jamming signal. These two components have the same signaling structure, and are separable at the intended receiver. Furthermore, the cooperative jamming signal is perfectly *aligned* with the message signal from the other transmitter (see Figure 10). Our converse starts with considering transmitter 2 as a helper for transmitter-receiver pair 1. In contrast to the single-message case, since transmitter 2 also intends to deliver a message W_2 to receiver 2, in the second step, we treat transmitter 1 as the helper for the transmitter-receiver pair 2 and upper bound the differential entropy of its channel input by using its relationship with the message rate of W_2. The converse matches the achievability lower bound, giving the exact secure d.o.f. for the two-user interference channel with confidential messages as $\frac{2}{3}$.

We then generalize this result to the case with one helper, i.e., two two-user Gaussian interference channel with confidential messages and one helper. We show that a sum secure d.o.f. of 1 is achievable. The structure of the channel inputs in the corresponding achievable scheme is simpler than in the cases of previous channel models. Each transmitter sends a signal carrying its message. With probability one, these two signals are not in the same *rational dimension* at the receivers. On the other hand, the cooperative jamming signal from the helper can be aligned with the unintended message at each receiver while leaving the intended message intact (see Figure 11). The converse for this case follows from the converse without any secrecy constraints for the two-user Gaussian interference channel [37], which is 1. This concludes that the exact sum secure d.o.f. of the two-user Gaussian interference channel with confidential messages and one helper is 1. Since utilizing one helper is sufficient to achieve the upper bound, the sum secure d.o.f. remains the same for arbitrary M helpers.

For the K-user multiple access wiretap channel, the best known lower bound for the sum secure d.o.f. is $\frac{K-1}{K}$ [29] which gives $\frac{1}{2}$ for $K = 2$. In addition, for $K = 2$, the individual secure d.o.f. of $\frac{1}{2}$ achieved in [33] and [28, Theorem 5.4 on page 126] in the context of the wiretap channel with a helper (for the class of algebraic irrational channel gains) can also be understood as a lower bound for the sum secure d.o.f. for the two-user multiple access wiretap channel. We show that, by using interference alignment and cooperative jamming at all transmitters simultaneously, we can achieve a sum secure d.o.f. of $\frac{K(K-1)}{K(K-1)+1}$ for the K-user multiple access wiretap channel, for *almost all channel gains*, which is better than all previously known achievable secure d.o.f. In particular, for $K = 2$, our achievable scheme gives a sum secure d.o.f. of $\frac{2}{3}$. In order to obtain this sum secure d.o.f., we need a more detailed structure for each channel input. Each transmitter sends a mixed signal containing the message signal and a cooperative jamming signal. Specifically, each transmitter divides its own message into $K-1$ sub-messages each of which having the same structure as the cooperative jamming signal. By such a scheme, the total K cooperative jamming signals from the K transmitters *span* the whole *space* at the eavesdropper's observation, in order to hide each one of the message signals from the eavesdropper. On the other hand, to maximize the sum secrecy d.o.f., the cooperative jamming signals from all of the transmitters are *aligned* in the same *dimension* at the legitimate receiver to occupy the smallest *space* (see Figure 12). Our converse is a generalization of our converse used in earlier channel model. We first show that the sum secrecy rate is upper bounded by the sum of differential entropies of all channel inputs except the one eliminated by the eavesdropper's observation. Then, we consider each channel input as the jamming signal for all other transmitters and upper bound its differential entropy by using its relationship with the sum rate of the messages belonging to all other transmitters. This gives us a matching converse and shows that the exact sum secure d.o.f. for this channel model is $\frac{K(K-1)}{K(K-1)+1}$.

2 System Model and Definitions

In this paper, we consider four fundamental channel models: wiretap channel with helpers, broadcast channel with confidential messages and helpers, two-user interference channel with confidential messages and helpers, and multiple access wiretap channel. In this section, we give the channel models and relevant definitions. All the channels are additive white Gaussian noise (AWGN) channels. All the channel gains are time-invariant, and independently drawn from continuous distributions.

2.1 Wiretap Channel with Helpers

The Gaussian wiretap channel with helpers (see Figure 2) is defined by,

$$Y_1 = h_1 X_1 + \sum_{j=2}^{M+1} h_j X_j + N_1 \tag{1}$$

$$Y_2 = g_1 X_1 + \sum_{j=2}^{M+1} g_j X_j + N_2 \tag{2}$$

where Y_1 is the channel output of the legitimate receiver, Y_2 is the channel output of the eavesdropper, X_1 is the channel input of the legitimate transmitter, X_i, for $i = 2, \ldots, M+1$, are the channel inputs of the M helpers, h_i is the channel gain of the ith transmitter to the legitimate receiver, g_i is the channel gain of the ith transmitter to the eavesdropper, and N_1 and N_2 are two independent zero-mean unit-variance Gaussian random variables. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, M+1$.

Transmitter 1 intends to send a message W, uniformly chosen from a set $\mathcal{W}$, to the legitimate receiver (receiver 1). The rate of the message is $R \triangleq \frac{1}{n} \log |\mathcal{W}|$, where n is the number of channel uses. Transmitter 1 uses a stochastic function $f : \mathcal{W} \to \mathbf{X}_1$ to encode the message, where $\mathbf{X}_1 \triangleq X_1^n$ is the n-length channel input.[2] The legitimate receiver decodes the message as $\hat{W}$ based on its observation $\mathbf{Y}_1$. A secrecy rate R is said to be achievable if for any $\epsilon > 0$ there exists an n-length code such that receiver 1 can decode this message reliably, i.e., the probability of decoding error is less than ϵ,

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

and the message is kept information-theoretically secure against the eavesdropper,

$$\frac{1}{n} H(W|\mathbf{Y}_2) \geq \frac{1}{n} H(W) - \epsilon \tag{4}$$

i.e., that the uncertainty of the message W, given the observation $\mathbf{Y}_2$ of the eavesdropper,

[2]We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_1 \triangleq X_1^n$, $\mathbf{Y}_1 \triangleq Y_1^n$, $\mathbf{Y}_2 \triangleq Y_2^n$, etc.

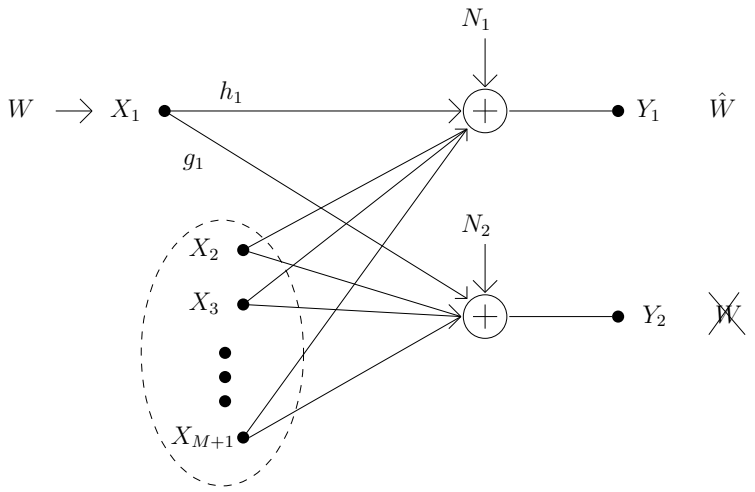

Figure 2: Gaussian wiretap channel with M helpers.

is almost equal to the entropy of the message. The supremum of all achievable secrecy rates is the secrecy capacity C_s and the secure d.o.f., D_s, is defined as

$$D_s \triangleq \lim_{P\to\infty} \frac{C_s}{\frac{1}{2}\log P} \tag{5}$$

Note that $D_s \leq 1$ is an upper bound. To avoid trivial cases, we assume that $h_1 \neq 0$ and $g_1 \neq 0$. Without the independent helpers, i.e., $M = 0$, the secrecy capacity of the Gaussian wiretap channel is known [3]

$$C_s = \frac{1}{2}\log\left(1 + h_1^2 P\right) - \frac{1}{2}\log\left(1 + g_1^2 P\right) \tag{6}$$

and from (5) the secure d.o.f. is zero. Therefore, we assume $M \geq 1$. If there exists a j ($j = 2, \ldots, M+1$) such that $h_j = 0$ and $g_j \neq 0$, then a lower bound of 1 secure d.o.f. can be obtained for this channel by letting this helper jam the eavesdropper by i.i.d. Gaussian noise of power P and keeping all other helpers silent. This lower bound matches the upper bound, giving the secure d.o.f. On the other hand, if there exists a j ($j = 2, \ldots, M+1$) such that $h_j \neq 0$ and $g_j = 0$, then this helper can be removed from the channel model without affecting the secure d.o.f. Therefore, in the rest of the paper, for the case of Gaussian wiretap channel with M helpers, we assume that $M \geq 1$ and $h_j \neq 0$ and $g_j \neq 0$ for all $j = 1, \cdots, M+1$.

2.2 Broadcast Channel with Confidential Messages and Helpers

The Gaussian broadcast channel with confidential messages and helpers (see Figure 3 for one helper) is defined by,

$$Y_1 = h_1 X_1 + \sum_{j=2}^{M+1} h_j X_j + N_1 \tag{7}$$

$$Y_2 = g_1 X_1 + \sum_{j=2}^{M+1} g_j X_j + N_2 \tag{8}$$

In this model, transmitter 1 has two independent messages, W_1 and W_2, intended for receivers 1 and 2, respectively. Messages W_1 and W_2 are independently and uniformly chosen from sets $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively. The rates of the messages are $R_1 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_1|$ and $R_2 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_2|$. Transmitter 1 uses a stochastic function $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathbf{X}_1$ to encode the messages. The messages are said to be confidential if only the intended receiver can decode each message, i.e., each receiver is an eavesdropper for the other. Transmitters $2, 3, \cdots, M+1$ are the independent helpers. Similar to (3) and (4), we define the reliability and secrecy of the messages as,

$$\Pr[W_1 \neq \hat{W}_1] \leq \epsilon \tag{9}$$

$$\Pr[W_2 \neq \hat{W}_2] \leq \epsilon \tag{10}$$

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1) - \epsilon \tag{11}$$

$$\frac{1}{n}H(W_2|\mathbf{Y}_1) \geq \frac{1}{n}H(W_2) - \epsilon \tag{12}$$

The sum secure d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{13}$$

where the supremum is over all achievable secrecy rate pairs (R_1, R_2).

2.3 Interference Channel with Confidential Messages and Helpers

The two-user Gaussian interference channel with confidential messages and helpers (see Figure 4) is defined by,

$$Y_1 = h_{1,1} X_1 + h_{2,1} X_2 + \sum_{j=3}^{M+2} h_{j,1} X_j + N_1 \tag{14}$$

$$Y_2 = h_{1,2} X_1 + h_{2,2} X_2 + \sum_{j=3}^{M+2} h_{j,2} X_j + N_2 \tag{15}$$

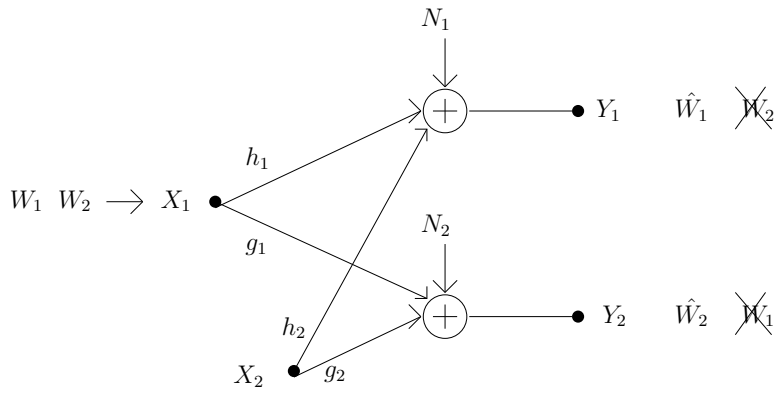

Figure 3: Gaussian broadcast channel with confidential messages and $M = 1$ helper.

where $X_1, X_2, \cdots, X_{M+2}, N_1$ and N_2 are mutually independent.

One special, but important, case is the two-user Gaussian interference channel with confidential messages, i.e., $M = 0$, which is shown in Figure 5 and defined by,

$$Y_1 = h_{1,1}X_1 + h_{2,1}X_2 + N_1 \tag{16}$$

$$Y_2 = h_{1,2}X_1 + h_{2,2}X_2 + N_2 \tag{17}$$

In the two-user interference channel with confidential messages, each transmitter wishes to send a confidential message to its own receiver. Transmitter 1 has message W_1 uniformly chosen from set $\mathcal{W}_1$. The rate of the message is $R_1 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_1|$. Transmitter 1 uses a stochastic function $f_1 : \mathcal{W}_1 \to \mathbf{X}_1$ to encode the message. Similarly, transmitter 2 has message W_2 (independent of W_1) uniformly chosen from set $\mathcal{W}_2$. The rate of the message is $R_2 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_2|$. Transmitter 2 uses a stochastic function $f_2 : \mathcal{W}_2 \to \mathbf{X}_2$ to encode the message. The messages are said to be confidential if only the intended receiver can decode each message, i.e., each receiver is an eavesdropper for the other. Transmitters $2, 3, \cdots, M+1$ are the independent helpers. Similar to (3) and (4), we define the reliability and secrecy of the messages as,

$$\Pr[W_1 \neq \hat{W}_1] \leq \epsilon \tag{18}$$

$$\Pr[W_2 \neq \hat{W}_2] \leq \epsilon \tag{19}$$

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1) - \epsilon \tag{20}$$

$$\frac{1}{n}H(W_2|\mathbf{Y}_1) \geq \frac{1}{n}H(W_2) - \epsilon \tag{21}$$

The sum secure d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{22}$$

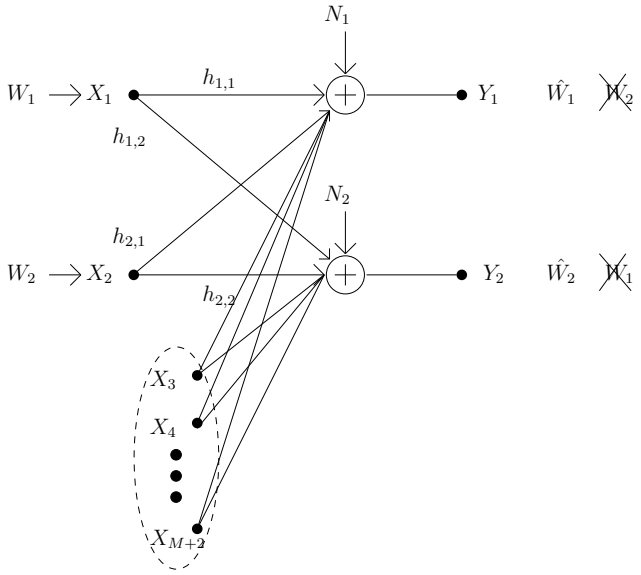

Figure 4: Two-user Gaussian interference channel with confidential messages and M helpers.

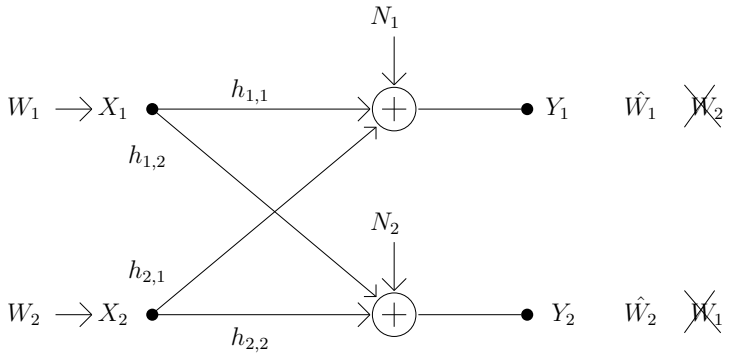

Figure 5: Two-user Gaussian interference channel with confidential messages.

where the supremum is over all achievable secrecy rate pairs (R_1, R_2).

2.4 Multiple Access Wiretap Channel

The K-user Gaussian multiple access wiretap channel (see Figure 6) is defined by,

$$Y_1 = \sum_{i=1}^{K} h_j X_j + N_1 \tag{23}$$

$$Y_2 = \sum_{i=1}^{K} g_j X_j + N_2 \tag{24}$$

In this channel model, each transmitter i has a message W_i intended for the legitimate receiver whose channel output is Y_1. All of the messages are independent. Message W_i is uniformly chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \triangleq \frac{1}{n} \log |\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ to encode its message. All of the messages are needed to

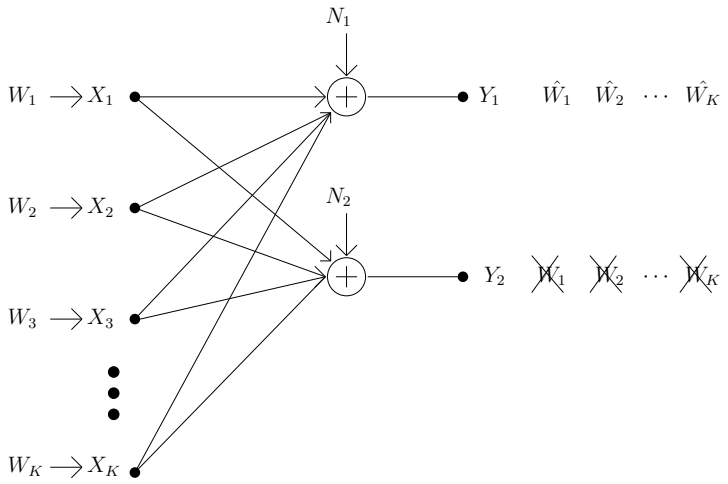

Figure 6: K-user multiple access wiretap channel.

be kept secret from the eavesdropper, whose channel output is Y_2.

Similar to (3), the reliability of the messages is defined by

$$\Pr\left[(W_1, \cdots, W_K) \neq (\hat{W}_1, \cdots, \hat{W}_K)\right] \leq \epsilon \tag{25}$$

and similar to (4) the secrecy constraint (for the entire message set) is defined as

$$\frac{1}{n} H(W_1, W_2, \cdots, W_K | \mathbf{Y}_2) \geq \frac{1}{n} H(W_1, W_2, \cdots, W_K) - \epsilon \tag{26}$$

Note that this definition implies the secrecy for any subset of the messages, including individual messages, i.e.,

$$\begin{aligned}
\frac{1}{n} H(W_{\mathbf{S}} | \mathbf{Y}_2) &= \frac{1}{n} H(W_1, W_2, \cdots, W_K | \mathbf{Y}_2) - \frac{1}{n} H(W_{\mathbf{S}^c} | \mathbf{Y}_2, W_{\mathbf{S}}) && (27)\\
&\geq \frac{1}{n} H(W_1, W_2, \cdots, W_K | \mathbf{Y}_2) - \frac{1}{n} H(W_{\mathbf{S}^c} | W_{\mathbf{S}}) && (28)\\
&\geq \frac{1}{n} H(W_1, W_2, \cdots, W_K) - \epsilon - \frac{1}{n} H(W_{\mathbf{S}^c} | W_{\mathbf{S}}) && (29)\\
&\geq \frac{1}{n} H(W_{\mathbf{S}}) - \epsilon && (30)
\end{aligned}$$

for any $\mathbf{S} \subset \{1, 2, \cdots, K\}$. The sum secure d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P \to \infty} \sup \frac{\sum_{i=1}^{K} R_i}{\frac{1}{2} \log P} \tag{31}$$

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

3 General Converse Results

In this section, we give two lemmas that will be used in the converse proofs in later sections.

3.1 Secrecy Penalty

Consider the channel model formulated in Section 2.1, where transmitter 1 wishes to have secure communication with receiver 1, in the presence of an eavesdropper (receiver 2) and M helpers (transmitters 2 through $M+1$). We propose a general upper bound for the secrecy rate between transmitter 1 and receiver 1 by working with n-letter signals, and introducing new mutually independent Gaussian random variables $\{\tilde{N}_i\}_{i=2}^{M}$ which are zero-mean and of variance $\tilde{\sigma}_i^2$ where $\tilde{\sigma}_i^2 < \min(1/h_i^2, 1/g_i^2)$, and are independent of all other random variables. Each vector $\tilde{\mathbf{N}}_i$ is an i.i.d. sequence of $\tilde{N}_i$.

In the following lemma, we give a general upper bound for the secrecy rate. This lemma states that the secrecy rate of the legitimate pair is upper bounded by the difference of the sum of differential entropies of all channel inputs (perturbed by small noise) and the differential entropy of the eavesdropper's observation; see (32). This upper bound can further be interpreted as follows: If we consider the eavesdropper's observation as the *secrecy penalty,* then the secrecy penalty is tantamount to the elimination of one of the channel inputs in the system; see (33).

Lemma 1 *The secrecy rate of the legitimate pair is upper bounded as*

$$nR \leq \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc \tag{32}$$

$$\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{33}$$

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

Proof: We use notation c_i, for $i \geq 1$, to denote constants which are independent of the power P. We start as follows:

$$nR = H(W) = H(W|\mathbf{Y}_1) + I(W; \mathbf{Y}_1) \tag{34}$$

$$\leq I(W; \mathbf{Y}_1) + nc_1 \tag{35}$$

$$\leq I(W; \mathbf{Y}_1) - I(W; \mathbf{Y}_2) + nc_2 \tag{36}$$

where we used Fano's inequality and the secrecy constraint in (4). By providing $\mathbf{Y}_2$ to receiver 1, we further upper bound nR as

$$\begin{aligned} nR &\leq I(W;\mathbf{Y}_1,\mathbf{Y}_2) - I(W;\mathbf{Y}_2) + nc_2 && (37)\\ &= I(W;\mathbf{Y}_1|\mathbf{Y}_2) + nc_2 && (38)\\ &= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2,W) + nc_2 && (39)\\ &\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && (40) \end{aligned}$$

where (40) is due to

$$\begin{aligned} h(\mathbf{Y}_1|\mathbf{Y}_2,W) &\geq h(\mathbf{Y}_1|\mathbf{X}_1,\mathbf{X}_2,\cdots,\mathbf{X}_{M+1},\mathbf{Y}_2,W) && (41)\\ &= h(\mathbf{N}_1|\mathbf{X}_1,\mathbf{X}_2,\cdots,\mathbf{X}_{M+1},\mathbf{Y}_2,W) && (42)\\ &= h(\mathbf{N}_1) && (43)\\ &= \frac{n}{2}\log 2\pi e && (44) \end{aligned}$$

which is independent of P.

In the next step, we introduce random variables $\tilde{\mathbf{X}}_i$ which are noisy versions of the channel inputs $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ for $i = 1, 2, \cdots, M+1$. Thus, starting from (40),

$$\begin{aligned} nR &\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && (45)\\ &= h(\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (46)\\ &= h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1},\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (47)\\ &\leq h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1},\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1,\mathbf{Y}_2,\mathbf{X}_1,\mathbf{X}_2,\cdots,\mathbf{X}_{M+1})\\ &\quad - h(\mathbf{Y}_2) + nc_3 && (48)\\ &\leq h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1},\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1,\tilde{\mathbf{N}}_2,\cdots,\tilde{\mathbf{N}}_{M+1}|\mathbf{Y}_1,\mathbf{Y}_2,\mathbf{X}_1,\mathbf{X}_2,\cdots,\mathbf{X}_{M+1})\\ &\quad - h(\mathbf{Y}_2) + nc_3 && (49)\\ &\leq h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1},\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1,\tilde{\mathbf{N}}_2,\cdots,\tilde{\mathbf{N}}_{M+1}) - h(\mathbf{Y}_2) + nc_3 && (50)\\ &\leq h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1},\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_4 && (51)\\ &= h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}) + h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_4 && (52)\\ &\leq h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_5 && (53)\\ &= \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc_5 && (54) \end{aligned}$$

where (53) is due to $h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\cdots,\tilde{\mathbf{X}}_{M+1}) \leq nc_6$. The intuition behind this is that, given all (slightly noisy versions of) the channel inputs, (at high SNR) the channel outputs

can be *reconstructed*. To show this formally, we have

$$
\begin{aligned}
&h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) \\
&\quad \le h(\mathbf{Y}_1|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) + h(\mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) && (55)\\
&\quad = h\left(\sum_{i=1}^{M+1} h_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}\right) \\
&\qquad + h\left(\sum_{i=1}^{M+1} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}\right) && (56)\\
&\quad = h\left(-\sum_{i=1}^{M+1} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}\right) \\
&\qquad + h\left(-\sum_{i=1}^{M+1} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}\right) && (57)\\
&\quad \le h\left(-\sum_{i=1}^{M+1} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1\right) + h\left(-\sum_{i=1}^{M+1} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2\right) && (58)\\
&\quad \stackrel{\triangle}{=} nc_6 && (59)
\end{aligned}
$$

which completes the proof of (32).

Finally, we show (33). To this end, fixing a j, which could be arbitrary, we express $\mathbf{Y}_2$ in a stochastically equivalent form $\tilde{\mathbf{Y}}_2$, i.e.,

$$\mathbf{Y}_2 = g_j\mathbf{X}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}_2 \tag{60}$$

$$\tilde{\mathbf{Y}}_2 = g_j\tilde{\mathbf{X}}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}_2' \tag{61}$$

have the same distribution, where $\mathbf{N}_2'$ is an i.i.d. sequence of a random variable N_2' which is Gaussian with zero-mean and variance $(1 - g_j^2\tilde{\sigma}_j^2)$, and is independent of all other random variables. Then, we have

$$
\begin{aligned}
h(\mathbf{Y}_2) &= h(\tilde{\mathbf{Y}}_2) && (62)\\
&= h\left(g_j\tilde{\mathbf{X}}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}_2'\right) && (63)\\
&\ge h\left(g_j\tilde{\mathbf{X}}_j\right) && (64)\\
&= n\log|g_j| + h(\tilde{\mathbf{X}}_j) && (65)
\end{aligned}
$$

where (64) is due to the differential entropy version of [38, Problem 2.14]. Substituting this into (32) gives us (33). ■

3.2 Role of a Helper

Intuitively, a cooperative jamming signal from a helper may potentially increase the secrecy of the legitimate transmitter-receiver pair by creating extra equivocation at the eavesdropper. However, if the helper creates too much equivocation, it may also hurt the decoding performance of the legitimate receiver. Since the legitimate receiver needs to decode message W by observing $\mathbf{Y}_1$, there must exist a constraint on the cooperative jamming signal of the helper. To this end, we develop a constraint on the differential entropy of (the noisy version of) the cooperative jamming signal of any given helper, helper j in (66), in terms of the differential entropy of the legitimate user's channel output and the message rate $H(W)$, in the following lemma. The inequality in this lemma, (66), can alternatively be interpreted as an upper bound on the message rate, i.e., on $H(W)$, in terms of the difference of the differential entropies of the channel output of the legitimate receiver and the channel input of the jth helper; in particular, the higher the differential entropy of the cooperative jamming signal the lower this upper bound will be. This motivates not using i.i.d. Gaussian cooperative jamming signals which have the highest differential entropy.

Finally, we note as an aside that, since this upper bound is derived based on the reliability of the legitimate user's decoding (not involving any secrecy constraints), it can be used in d.o.f. calculations in settings not involving secrecy. We show an application of this lemma in a non-secrecy context by developing an alternative proof for the multiplexing gain of the K-user Gaussian interference channel, which was originally proved in [37], in Appendix A.

Lemma 2 *For reliable decoding at the legitimate receiver, the differential entropy of the input signal of helper j, $\mathbf{X}_j$, must satisfy*

$$h(\mathbf{X}_j + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_1) - H(W) + nc \tag{66}$$

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

Proof: To reliably decode the message at the legitimate receiver, we must have

$$\begin{aligned}
nR = H(W) &\leq I(\mathbf{X}_1; \mathbf{Y}_1) && (67)\\
&= h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\mathbf{X}_1) && (68)\\
&= h(\mathbf{Y}_1) - h\left(\sum_{i=2}^{M+1} h_i \mathbf{X}_i + \mathbf{N}_1\right) && (69)\\
&\leq h(\mathbf{Y}_1) - h\left(h_j \mathbf{X}_j + \mathbf{N}_1\right) && (70)\\
&\leq h(\mathbf{Y}_1) - h\left(h_j \mathbf{X}_j + h_j \tilde{\mathbf{N}}\right) && (71)\\
&= h(\mathbf{Y}_1) - h\left(\mathbf{X}_j + \tilde{\mathbf{N}}\right) + nc && (72)
\end{aligned}$$

where (70) and (71) are due to the differential entropy version of [38, Problem 2.14]. In going from (70) to (71), we also used the infinite divisibility of Gaussian distribution and expressed $\mathbf{N}_1$ in its stochastically equivalent form as $\mathbf{N}_1 = h_j\tilde{\mathbf{N}} + \mathbf{N}'$ where $\mathbf{N}'$ is an i.i.d. sequence of random variable N' which is Gaussian with zero-mean and appropriate variance, and which is independent of all other random variables. ■

Note that, although we develop the inequality in (66) for the message of transmitter-receiver pair 1, this result also holds for the message of any transmitter-receiver pair in a multiple-message setting provided that the zero-mean Gaussian noise $\tilde{N}$ has an appropriately small variance.

4 Wiretap Channel with One Helper

In this section, we consider the Gaussian wiretap channel with one helper as formulated in Section 2.1 for the case $M = 1$. In this section, we will show that the secure d.o.f. is $\frac{1}{2}$ for almost all channel gains as stated in the following theorem. The converse follows from the general secrecy penalty upper bound in Section 3.1 and the cooperative jamming signal upper bound in Section 3.2. The achievability is based on cooperative jamming with discrete signaling and real interference alignment.

Theorem 1 *The secure d.o.f. of the Gaussian wiretap channel with one helper is $\frac{1}{2}$ with probability one.*

4.1 Converse

We start with (33) of Lemma 1 with $M = 1$ and by choosing $j = 1$,

$$nR \leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{73}$$

$$= h(\tilde{\mathbf{X}}_2) + nc' \tag{74}$$

$$\leq h(\mathbf{Y}_1) - H(W) + nc_7 \tag{75}$$

$$\leq \frac{n}{2}\log P - H(W) + nc_8 \tag{76}$$

where (75) is due to Lemma 2. By noting $H(W) = nR$ and using (5), (76) implies that

$$D_s \leq \frac{1}{2} \tag{77}$$

which concludes the converse part of the theorem.

4.2 Achievable Scheme

To show the achievability by interference alignment, we slightly change the notation. Let $\bar{X}_1 \triangleq g_1 X_1$, $\bar{X}_2 \triangleq g_2 X_2$, $\alpha \triangleq h_1/g_1$, and $\beta \triangleq h_2/g_2$. Then, the channel model becomes

$$Y_1 = \alpha \bar{X}_1 + \beta \bar{X}_2 + N_1 \tag{78}$$

$$Y_2 = \bar{X}_1 + \bar{X}_2 + N_2 \tag{79}$$

Here $\bar{X}_1$ is the input signal carrying the message W of the legitimate transmitter and $\bar{X}_2$ is the cooperative jamming signal from the helper. Our goal is to properly design $\bar{X}_1$ and $\bar{X}_2$ such that they are distinguishable at the legitimate receiver, meanwhile they align together at the eavesdropper. To prevent decoding of the message signal at the eavesdropper, we need to make sure that the cooperative jamming signal occupies the same *dimensions* as the message signal at the eavesdropper; on the other hand, we need to make sure that the legitimate receiver is able to decode $\bar{X}_2$, which in fact, is not useful. Intuitively, secrecy penalty is almost *half* of the signal space, and we should be able to have a secure d.o.f. of $\frac{1}{2}$. This is illustrated in Figure 7, and proved formally in the sequel.

We choose both of the input symbols $\bar{X}_1$ and $\bar{X}_2$ independent and uniformly distributed over the same PAM constellation

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{80}$$

where Q is a positive integer and a is a real number used to normalize the transmission power, and is also the minimum distance between the points belonging to $C(a, Q)$.

Since $\bar{\mathbf{X}}_2$ is an i.i.d. sequence and is independent of $\bar{\mathbf{X}}_1$, the following secrecy rate is always achievable [1]

$$C_s \geq I(\bar{X}_1; Y_1) - I(\bar{X}_1; Y_2) \tag{81}$$

In order to show that $D_s \geq \frac{1}{2}$, it suffices to prove that this lower bound provides $\frac{1}{2}$ secure d.o.f. To this end, we need to find a lower bound for $I(\bar{X}_1; Y_1)$ and an upper bound for $I(\bar{X}_1; Y_2)$. It is clear that

$$H(\bar{X}_1) = H(\bar{X}_2) = \log |C(a, Q)| = \log(2Q+1) \tag{82}$$

Also, note that, besides the additive Gaussian noise, the observation at receiver 1 is a linear combination of $\bar{X}_1$ and $\bar{X}_2$, i.e.,

$$Y_1 - N_1 = \alpha \bar{X}_1 + \beta \bar{X}_2 \tag{83}$$

where α and β are rationally independent real numbers[3] with probability 1.

[3] $a_1, a_2, \ldots, a_L$ are rationally independent if whenever $q_1, q_2, \ldots, q_L$ are rational numbers then $\sum_{i=1}^{L} q_i a_i = 0$ implies $q_i = 0$ for all i.

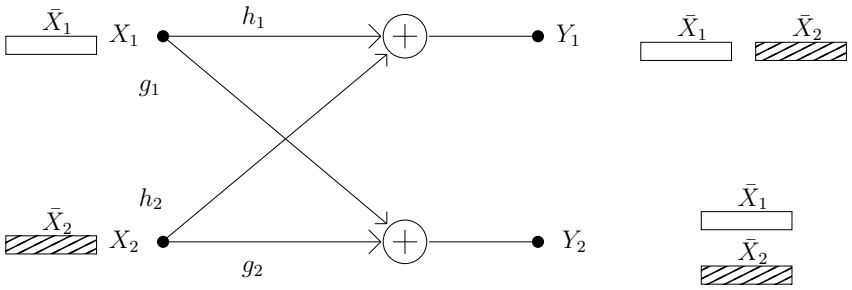

Figure 7: Illustration of interference alignment for the Gaussian wiretap channel with one helper.

The space observed at receiver 1 consists of $(2Q+1)^2$ signal points. By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, references [34, 35] bounded the minimum distance d_{min} between the points in receiver 1's constellation as follows: For any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{Q^{1+\delta}} \tag{84}$$

for almost all rationally independent $\{\alpha, \beta\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as follows,

$$\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8Q^{2(1+\delta)}}\right) \tag{85}$$

where $\hat{X}_1$ is the estimate for $\bar{X}_1$ obtained by choosing the closest point in the constellation based on observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(2+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P, then

$$\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 P}{8Q^{2(1+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right) \tag{86}$$

and we can have $\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose $\gamma \leq \min(|g_1|, |g_2|)$. By Fano's inequality and the Markov chain $\bar{X}_1 \to Y_1 \to \hat{X}_1$, we know that

$$H(\bar{X}_1|Y_1) \leq H(\bar{X}_1|\hat{X}_1) \tag{87}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right) \log(2Q+1) \tag{88}$$

which means that

$$I(\bar{X}_1;Y_1) = H(\bar{X}_1) - H(\bar{X}_1|Y_1) \tag{89}$$
$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right)\right] \log(2Q+1) - 1 \tag{90}$$

On the other hand,

$$I(\bar{X}_1;Y_2) \leq I(\bar{X}_1; \bar{X}_1 + \bar{X}_2) \tag{91}$$
$$= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2|\bar{X}_1) \tag{92}$$
$$= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2) \tag{93}$$
$$\leq \log(4Q+1) - \log(2Q+1) \tag{94}$$
$$\leq \log \frac{4Q+1}{2Q+1} \tag{95}$$
$$\leq 1 \tag{96}$$

where (94) is due to the fact that entropy of the sum $\bar{X}_1 + \bar{X}_2$ is maximized by the uniform distribution which takes values over a set of cardinality $4Q+1$.

Combining (90) and (96), we have

$$C_s \geq I(\bar{X}_1;Y_1) - I(\bar{X}_1;Y_2) \tag{97}$$
$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right)\right] \log(2Q+1) - 2 \tag{98}$$
$$= \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right)\right] \log\left(2P^{\frac{1-\delta}{2(2+\delta)}} + 1\right) - 2 \tag{99}$$
$$= \frac{1-\delta}{(2+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{100}$$

where the $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{1}{2}$ secure d.o.f., which concludes the achievability part of the theorem.

5 Wiretap Channel with M Helpers

In this section, we consider the Gaussian wiretap channel with M helpers as formulated in Section 2.1 for general $M > 1$. In this section, we will show that the secure d.o.f. is $\frac{M}{M+1}$ for almost all channel gains as stated in the following theorem. This shows that even though the helpers are independent, the secure d.o.f. increases monotonically with the number of helpers M. The converse follows from the general secrecy penalty upper bound in Section 3.1 and the cooperative jamming signal upper bound in Section 3.2. The achievability is based on cooperative jamming of M helpers with discrete signaling and real interference alignment.

Theorem 2 *The secure d.o.f. of the Gaussian wiretap channel with M helpers is $\frac{M}{M+1}$ with probability one.*

5.1 Converse

We again start with (33) of Lemma 1 with the selection of $j = 1$

$$nR \leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{101}$$

$$= \sum_{i=2}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{102}$$

$$\leq M[h(\mathbf{Y}_1) - H(W)] + nc_9 \tag{103}$$

where (103) is due to Lemma 2 for each jamming signal $\tilde{\mathbf{X}}_i$, $i = 2, 3, \cdots, M+1$. By noting $H(W) = nR$, (103) implies that

$$(M+1)nR \leq Mh(\mathbf{Y}_1) + nc_9 \tag{104}$$

$$\leq M\left(\frac{n}{2}\log P\right) + nc_{10} \tag{105}$$

which further implies from (5) that

$$D_s \leq \frac{M}{M+1} \tag{106}$$

which concludes the converse part of the theorem.

5.2 Achievable Scheme

Let $\{V_2, V_3, \cdots, V_{M+1}, U_2, U_3, \cdots, U_{M+1}\}$ be mutually independent discrete random variables, each of which uniformly drawn from the same PAM constellation $C(a, Q)$, where a and Q will be specified later. We choose the input signal of the legitimate transmitter as

$$X_1 = \sum_{k=2}^{M+1} \frac{g_k}{g_1 h_k} V_k \tag{107}$$

and the input signal of the jth helper, $j = 2, 3, \cdots, M+1$, as

$$X_j = \frac{1}{h_j} U_j \tag{108}$$

Then, the observations of the receivers are

$$Y_1 = \sum_{k=2}^{M+1} \frac{h_1 g_k}{g_1 h_k} V_k + \left(\sum_{j=2}^{M+1} U_j \right) + N_1 \tag{109}$$

$$Y_2 = \sum_{k=2}^{M+1} \frac{g_k}{h_k} \Big(V_k + U_k \Big) + N_2 \tag{110}$$

The intuition here is as follows. We use M independent sub-signals V_k, $k = 2, 3, \cdots, M+1$, to represent the original message W. The input signal X_1 is a linear combination of V_ks. To cooperatively jam the eavesdropper, each helper k aligns the cooperative jamming signal U_k in the same *dimension* as the sub-signal V_k at the eavesdropper. At the legitimate receiver, all of the cooperative jamming signals U_ks are well-aligned such that they occupy a small portion of the signal space. Since, with probability one, $\left\{1, \frac{h_1 g_2}{g_1 h_2}, \frac{h_1 g_3}{g_1 h_3}, \cdots, \frac{h_1 g_{M+1}}{g_1 h_{M+1}}\right\}$ are rationally independent, the signals $\left\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=2}^{M+1} U_j\right\}$ can be distinguished by the legitimate receiver. As an example, the case of $M = 2$ is shown in Figure 8.

Since, for each $j \neq 1$, $\mathbf{X}_j$ is an i.i.d. sequence and independent of $\mathbf{X}_1$, the following secrecy rate is achievable [1]

$$C_s \geq I(X_1; Y_1) - I(X_1; Y_2) \tag{111}$$

Now, we first bound the probability of decoding error. Note that the *space* observed at receiver 1 consists of $(2Q+1)^M(2MQ+1)$ points in $M+1$ *dimensions*, and the sub-signal in each *dimension* is drawn from a constellation of $C(a, MQ)$. Here, we use the property that $C(a, Q) \subset C(a, MQ)$. By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, we can bound the minimum distance d_{min} between the points in receiver 1's *space* as follows: For any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{(MQ)^{M+\delta}} \tag{112}$$

for almost all rationally independent $\left\{1, \frac{h_1 g_2}{g_1 h_2}, \frac{h_1 g_3}{g_1 h_3}, \cdots, \frac{h_1 g_{M+1}}{g_1 h_{M+1}}\right\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1,

$$\Pr\left[X_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(MQ)^{2(M+\delta)}}\right) \tag{113}$$

where $\hat{X}_1$ is the estimate of X_1 by choosing the closest point in the constellation based on observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a

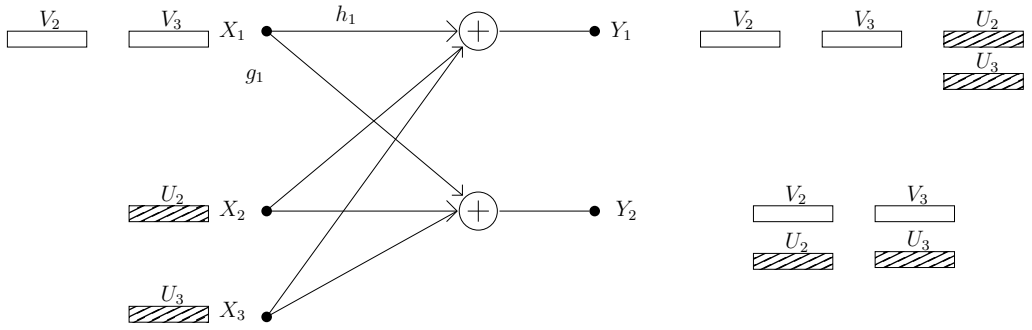

Figure 8: Illustration of interference alignment for the Gaussian wiretap channel with M helpers. Here, $M = 2$.

constant independent of P, then

$$\Pr\left[X_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P}{8(MQ)^{2(M+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right) \tag{114}$$

and we can have $\Pr\left[X_1 \neq \hat{X}_1\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose $\gamma \leq \min([\sum_{k=2}^{M+1}(\frac{g_k}{g_1 h_k})^2]^{-1/2}, |h_2|, |h_3|, \cdots, |h_{M+1}|)$. By Fano's inequality and the Markov chain $X_1 \to Y_1 \to \hat{X}_1$, we know that

$$H(X_1|Y_1) \leq H(X_1|\hat{X}_1) \tag{115}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right) \log(2Q+1)^M \tag{116}$$

which means that

$$I(X_1; Y_1) = H(X_1) - H(X_1|Y_1) \tag{117}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right)\right] \log(2Q+1)^M - 1 \tag{118}$$

On the other hand,

$$I(X_1;Y_2) \leq I\left(X_1; \sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) \tag{119}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\Big|X_1\right) \tag{120}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}U_k\right) \tag{121}$$

$$\leq \log(4Q+1)^M - \log(2Q+1)^M \tag{122}$$

$$\leq M \log \frac{4Q+1}{2Q+1} \tag{123}$$

$$\leq M \tag{124}$$

where (122) is due to the fact that entropy of the sum $\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)$ is maximized by the uniform distribution which takes values over a set of cardinality $(4Q+1)^M$.

Combining (118) and (124), we have

$$C_s \geq I(X_1;Y_1) - I(X_1;Y_2) \tag{125}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right)\right] \log(2Q+1)^M - (M+1) \tag{126}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right)\right] \log(2P^{\frac{1-\delta}{2(M+1+\delta)}}+1)^M - (M+1) \tag{127}$$

$$= \frac{M(1-\delta)}{(M+1+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{128}$$

where $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{M}{M+1}$ secure d.o.f., which concludes the achievability part of the theorem.

6 Broadcast Channel with Confidential Messages and M Helpers

In this section, we consider the Gaussian broadcast channel with confidential messages and M helpers formulated in Section 2.2. When there are no helpers, i.e., $M = 0$, due to the degradedness of the underlying Gaussian broadcast channel, one of the users (stronger) has the secrecy capacity which is equal to the secrecy capacity of the Gaussian wiretap channel, and the other user (weaker) has zero secrecy capacity. Therefore, for both users, the secure d.o.f. is zero, implying that the sum secure d.o.f. of the system is zero. Therefore, we consider the case $M \geq 1$. In this section, we will show that the sum secure d.o.f. is 1 for any $M \geq 1$, as stated in the following theorem.

Theorem 3 *The sum secure d.o.f. of the Gaussian broadcast channel with confidential mes-*

sages and $M \geq 1$ helpers is 1 with probability one.

6.1 Converse

An immediate upper bound for the secure d.o.f. of this problem is 1, i.e., $D_{s,\Sigma} \leq 1$ for any M. This comes from the fact that the d.o.f. for the Gaussian broadcast channel without any secrecy constraints is 1, and this constitutes an upper for the sum secure d.o.f. also.

6.2 Achievable Scheme

In the following, we will show that a sum secure d.o.f. of 1 can be achieved for the case of $M = 1$. Since the achievable scheme with a single helper achieves the upper bound $D_{s,\Sigma} \leq 1$, the sum secure d.o.f. for all $M \geq 1$ is 1. Therefore, if we have more than one helper, then all but one helper may remain silent.

We use the equivalent channel expression in (78) and (79). Let V_1, V_2 and U be three mutually independent random variables which are identically and uniformly distributed over the constellation $C(a, Q)$, where a and Q will be specified later. We assign channel inputs as $\bar{X}_1 = V_1 + \frac{\beta}{\alpha}V_2$ and $\bar{X}_2 = U$. Then, the observations at the two receivers are:

$$Y_1 = \alpha V_1 + \beta(V_2 + U) + N_1 \tag{129}$$

$$Y_2 = (V_1 + U) + \frac{\beta}{\alpha}V_2 + N_2 \tag{130}$$

We use two independent variables V_1 and V_2 to carry the messages W_1 and W_2 that go to the two receivers. In order to ensure that the messages are kept secure against the unintended receiver, we align the cooperative noise signal U from the helper in the *dimension* of V_2 at receiver 1, and in the *dimension* of V_1 at receiver 2. This is illustrated in Figure 9.

Since $\bar{\mathbf{X}}_2$ is an i.i.d. sequence, the following secrecy rate pair is achievable [4, Theorem 4]

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{131}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{132}$$

By using Khintchine-Groshev theorem, it is easy to verify that receiver i can decode V_i, for $i = 1, 2$ with arbitrarily small probability of decoding error with probability one, i.e., for any $\delta > 0$, there exists a constant k_δ such that the minimum distance d_{min} between points at receiver i is,

$$d_{min} \geq \frac{k_\delta a}{(2Q)^{1+\delta}} \tag{133}$$

for almost all rationally independent $\{\alpha, \beta\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error for such a PAM scheme by considering

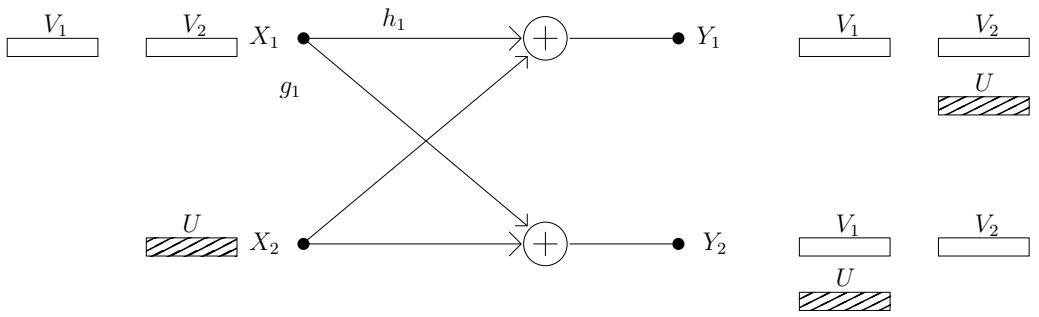

Figure 9: Illustration of interference alignment for the Gaussian broadcast channel with confidential messages and one helper.

the additive Gaussian noise at receiver i as,

$$\Pr\left[V_i \neq \hat{V}_i\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(2Q)^{2(1+\delta)}}\right) \tag{134}$$

where $\hat{V}_i$ is the estimate for V_i by choosing the closest point in the constellation based on observation Y_i. For any $\delta > 0$, if $Q = P^{\frac{1-\delta}{2(2+\delta)}}$, $a = \gamma P^{\frac{1}{2}}/Q$, and γ is a positive constant satisfying

$$\gamma \leq \min\left\{|g_1|\left[1+\left(\frac{\beta}{\alpha}\right)^2\right]^{-1/2}, |g_2|\right\} \tag{135}$$

then

$$\Pr\left[V_i \neq \hat{V}_i\right] \leq \exp\left(-\frac{4k_\delta^2\gamma^2 P}{8(2Q)^{2(2+\delta)}}\right) = \exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{2^{2\delta+5}}\right) \tag{136}$$

and we can have $\Pr\left[V_i \neq \hat{V}_i\right] \to 0$ as $P \to \infty$. By Fano's inequality and the Markov chain $V_i \to Y_i \to \hat{V}_i$, we know that

$$H(V_i|Y_i) \leq H(V_i|\hat{V}_i) \tag{137}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{2^{2\delta+5}}\right)\log(2Q+1) \tag{138}$$

which means that

$$I(V_i;Y_i) = H(V_i) - H(V_i|Y_i) \tag{139}$$

$$\geq \left[1-\exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{2^{2\delta+5}}\right)\right]\log(2Q+1) - 1 \tag{140}$$

$$= \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{141}$$

for $i = 1$ or 2.

On the other hand, for $i = 1$, we have

$$I(V_1; Y_2|V_2) \leq I\left(V_1; V_1 + U + \frac{\beta}{\alpha}V_2 \middle| V_2\right) \tag{142}$$

$$= H(V_1 + U) - H(U) \tag{143}$$

$$\leq 1 \tag{144}$$

Similarly, for $i = 2$, we have

$$I(V_2; Y_1|V_1) \leq I\left(V_2; \alpha V_1 + \beta(V_2 + U) \middle| V_1\right) \tag{145}$$

$$= H(V_2 + U) - H(U) \tag{146}$$

$$\leq 1 \tag{147}$$

which implies that the following sum secrecy rate is achievable

$$R_1 + R_2 \geq \frac{2 - 2\delta}{2 + \delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{148}$$

If we choose δ small enough, then we can have $D_{s,\Sigma} \geq 1$. Combining this with the upper bound $D_{s,\Sigma} \leq 1$, we conclude that

$$D_{s,\Sigma} = 1 \tag{149}$$

with probability one.

7 Two-User Interference Channel with Confidential Messages and No Helpers

In this section, we consider the two-user Gaussian interference channel with confidential messages formulated in Section 2.3 for the case of no helpers, i.e., $M = 0$. The case of $M \geq 1$ will be presented in Section 8. For the case of no helpers, we show that the sum secure d.o.f. is $\frac{2}{3}$ as stated in the following theorem.

Theorem 4 *The sum secure d.o.f. of the two-user Gaussian interference channel with confidential messages is $\frac{2}{3}$ with probability one.*

7.1 Converse

We first start with (32) of Lemma 1 to upper bound the individual rate R_1 of message W_1

$$nR_1 \leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) - h(\mathbf{Y}_2) + nc \tag{150}$$
$$\leq h(\tilde{\mathbf{X}}_1) + h(\mathbf{Y}_1) - H(W_1) - h(\mathbf{Y}_2) + nc_{11} \tag{151}$$
$$\leq h(\mathbf{Y}_2) - H(W_2) + h(\mathbf{Y}_1) - H(W_1) - h(\mathbf{Y}_2) + nc_{12} \tag{152}$$

where (151) is due to applying Lemma 2 for $h(\tilde{\mathbf{X}}_2)$ and (152) is due to applying Lemma 2 once again for $h(\tilde{\mathbf{X}}_1)$. By noting that $H(W_1) = nR_1$ and $H(W_2) = nR_2$, from (152), we have

$$2nR_1 + nR_2 \leq h(\mathbf{Y}_1) + nc_{12} \tag{153}$$

We use the same method to get a symmetric upper bound on the individual rate R_2 of message W_2 as

$$nR_1 + 2nR_2 \leq h(\mathbf{Y}_2) + nc_{13} \tag{154}$$

Then, combining (153) and (154), we get

$$3(nR_1 + nR_2) \leq h(\mathbf{Y}_1) + h(\mathbf{Y}_2) + nc_{14} \tag{155}$$
$$\leq 2\left(\frac{n}{2}\log P\right) + nc_{15} \tag{156}$$

which means

$$D_{s,\Sigma} \leq \frac{2}{3} \tag{157}$$

which concludes the converse part of the theorem.

7.2 Achievable Scheme

Let $\{V_1, U_1, V_2, U_2\}$ be mutually independent discrete random variables. Each of them is uniformly and independently drawn from the same constellation $C(a, Q)$, where a and Q will be specified later. Here, the role of V_i is to carry message W_i, and the role of U_i is the cooperative jamming signal to help the transmitter-receiver pair $j \neq i$. We choose the input signals of the transmitters as:

$$X_1 = V_1 + \frac{h_{2,1}}{h_{1,1}}U_1 \tag{158}$$
$$X_2 = V_2 + \frac{h_{1,2}}{h_{2,2}}U_2 \tag{159}$$

With these input signal selections, observations of the receivers are

$$Y_1 = h_{1,1}V_1 + h_{2,1}\big(U_1 + V_2\big) + \frac{h_{2,1}h_{1,2}}{h_{2,2}}U_2 + N_1 \tag{160}$$

$$Y_2 = h_{2,2}V_2 + h_{1,2}\big(U_2 + V_1\big) + \frac{h_{2,1}h_{1,2}}{h_{1,1}}U_1 + N_2 \tag{161}$$

Since, for each i and $j \neq i$, V_i and U_i are not in the same *dimension* at both receivers, we align U_i in the *dimension* of V_j at receiver i such that V_j is *secure* and V_i can occupy a *larger* space. This is illustrated in Figure 10.

By [4, Theorem 2], we know that the following secrecy rate pair is achievable

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{162}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{163}$$

For receiver 1, by using the Khintchine-Groshev theorem of Diophantine approximation in number theory, we can bound the minimum distance d_{min} between points in the receiver's *space*, i.e., for any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{(2Q)^{2+\delta}} \tag{164}$$

for almost all rationally independent $\left\{h_{1,1}, h_{2,1}, \frac{h_{2,1}h_{1,2}}{h_{2,2}}\right\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as,

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(2Q)^{2(2+\delta)}}\right) \tag{165}$$

where $\hat{V}_1$ is the estimate of V_1 by choosing the closest point in the constellation based on observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where

$$\gamma < \min_i \frac{1}{\sqrt{1 + \left(\frac{h_{j,i}}{h_{i,i}}\right)^2}} \tag{166}$$

is a constant independent of P to normalize the average power of the input signals. Then,

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 4P}{8(2Q)^{2(2+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+7}}\right) \tag{167}$$

and we can have $\Pr\left[V_1 \neq \hat{V}_1\right] \to 0$ as $P \to \infty$.

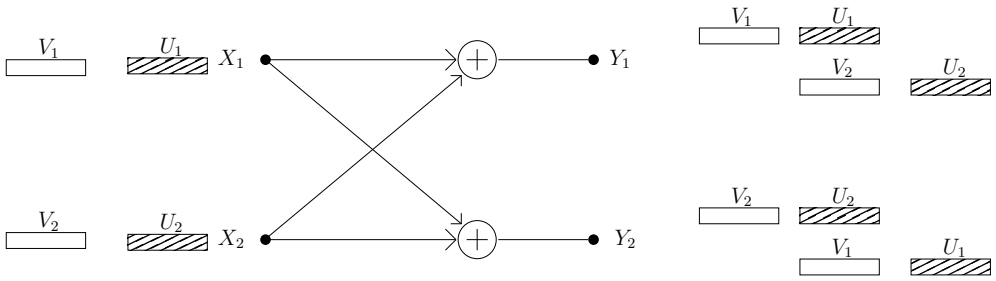

Figure 10: Illustration of interference alignment for the two-user Gaussian interference channel with confidential messages (no helpers).

To lower bound the achievable rate R_1, we first note that

$$\begin{aligned} I(V_1;Y_1) &\geq I(V_1;\hat{V}_1) && (168)\\ &= H(V_1) - H(V_1|\hat{V}_1) && (169)\\ &\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+7}}\right)\right] \log(2Q+1) - 1 && (170)\\ &= \frac{1-\delta}{3+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (171) \end{aligned}$$

On the other hand,

$$\begin{aligned} I(V_1;Y_2|V_2) &\leq I(V_1;Y_2,U_1|V_2) && (172)\\ &= I(V_1;Y_2|V_2,U_1) && (173)\\ &\leq I\left(V_1;h_{1,2}(U_2+V_1)|V_2,U_1\right) && (174)\\ &= H(U_2+V_1) - H(U_2) && (175)\\ &\leq \log(4Q+1) - \log(2Q+1) && (176)\\ &\leq 1 && (177) \end{aligned}$$

Combining (171) and (177), we obtain

$$\begin{aligned} R_1 &\geq I(V_1;Y_1) - I(V_1;Y_2|V_2) && (178)\\ &\geq \frac{1-\delta}{3+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (179) \end{aligned}$$

By applying this same analysis to rate R_2, we can obtain a symmetric result for R_2. Then, by choosing δ arbitrarily small, we can achieve $\frac{2}{3}$ sum secure d.o.f.

8 Two-User Interference Channel with Confidential Messages and M Helpers

In this section, we consider the two-user Gaussian interference channel with confidential messages formulated in Section 2.3 for the general case of $M \geq 1$ helpers. For this general case, we show that the sum secure d.o.f. is 1 as stated in the following theorem.

Theorem 5 *The sum secure d.o.f. of the two-user Gaussian interference channel with confidential messages and $M \geq 1$ helpers is 1 with probability one.*

8.1 Converse

An immediate upper bound for the secure d.o.f. of this problem is 1, i.e., $D_{s,\Sigma} \leq 1$ for any M. This comes from the fact that the d.o.f. for the two-user interference channel without any secrecy constraints is 1, and this constitutes an upper for the sum secure d.o.f. also. The fact that the d.o.f. of the two-user interference channel is 1 was first proved in [37]. We provide an alternative proof to this fact using the techniques developed in this paper in Appendix A.

8.2 Achievable Scheme

In the following, we will show that a sum secure d.o.f. of 1 can be achieved for the case of $M = 1$. Since the achievable scheme with a single helper achieves the upper bound $D_{s,\Sigma} \leq 1$, the sum secure d.o.f. for all $M \geq 1$ is 1. Therefore, if we have more than one helpers, then all but one helper may remain silent.

Let $\{V_1, V_2, U\}$ be mutually independent discrete random variables. Each of them is uniformly and independently drawn from the same constellation $C(a, Q)$, where a and Q will be specified later. Here, the role of V_i is to carry message W_i, and the role of U is the cooperative jamming signal from the helper. We choose the input signals of the transmitters as:

$$X_1 = \frac{h_{3,2}}{h_{1,2}} V_1 \tag{180}$$

$$X_2 = \frac{h_{3,1}}{h_{2,1}} V_2 \tag{181}$$

$$X_3 = U \tag{182}$$

With these input signal selections, observations of the receivers are

$$Y_1 = \frac{h_{3,2}h_{1,1}}{h_{1,2}}V_1 + h_{3,1}\big(U + V_2\big) + N_1 \tag{183}$$

$$Y_2 = \frac{h_{3,1}h_{2,2}}{h_{2,1}}V_2 + h_{3,2}\big(U + V_1\big) + N_2 \tag{184}$$

For each i and $j \neq i$, we align U in the *dimension* of V_j at receiver i such that V_j is *secure* and V_i can be decoded. This is illustrated in Figure 11.

Since $\mathbf{U}$ is an i.i.d. sequence, by [4, Theorem 2], we know that the following secrecy rate pair is achievable

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{185}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{186}$$

For receiver 1, by using the Khintchine-Groshev theorem of Diophantine approximation in number theory, we can bound the minimum distance d_{min} between the points in receiver's *space*, i.e., for any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{(2Q)^{1+\delta}} \tag{187}$$

for almost all rationally independent $\left\{\frac{h_{3,2}h_{1,1}}{h_{1,2}}, h_{3,1}\right\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as,

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(2Q)^{2(1+\delta)}}\right) \tag{188}$$

where $\hat{V}_1$ is the estimate of V_1 by choosing the closest point in the constellation based on the observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(2+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where

$$\gamma < \min\left(\left|\frac{h_{3,2}}{h_{1,2}}\right|^{-1}, \left|\frac{h_{3,1}}{h_{2,1}}\right|^{-1}, 1\right) \tag{189}$$

is a constant independent of P to normalize the average power of the input signals. Then,

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 4P}{8(2Q)^{2(1+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+5}}\right) \tag{190}$$

and we can have $\Pr\left[V_1 \neq \hat{V}_1\right] \to 0$ as $P \to \infty$.

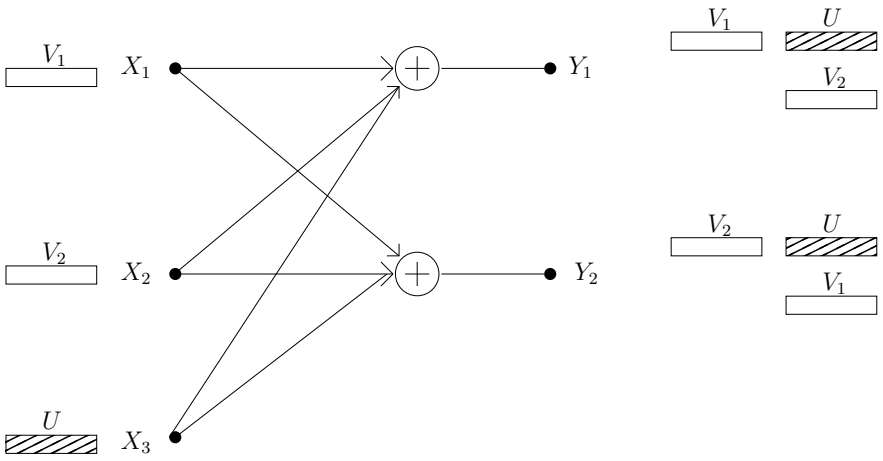

Figure 11: Illustration of interference alignment for the two-user Gaussian interference channel with confidential messages and one helper.

To lower bound the achievable rate R_1, we first note that

$$\begin{aligned} I(V_1;Y_1) &\geq I(V_1;\hat{V}_1) && (191)\\ &= H(V_1) - H(V_1|\hat{V}_1) && (192)\\ &\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{2^{2\delta+5}}\right)\right] \log(2Q+1) - 1 && (193)\\ &= \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (194) \end{aligned}$$

On the other hand,

$$\begin{aligned} I(V_1;Y_2|V_2) &\leq I\Big(V_1; h_{3,2}(U+V_1)|V_2\Big) && (195)\\ &= H(U+V_1) - H(U) && (196)\\ &\leq \log(4Q+1) - \log(2Q+1) && (197)\\ &\leq 1 && (198) \end{aligned}$$

Combining (194) and (198), we obtain

$$\begin{aligned} R_1 &\geq I(V_1;Y_1) - I(V_1;Y_2|V_2) && (199)\\ &\geq \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (200) \end{aligned}$$

By applying this same analysis to rate R_2, we can obtain a symmetric result for R_2. Then, by choosing δ arbitrarily small, we can achieve 1 sum secure d.o.f. with probability one for almost all channel gains for the $M = 1$ case.

9 K-User Multiple Access Wiretap Channel

In this section, we consider the K-user multiple access wiretap channel formulated in Section 2.4. We show that the sum secure d.o.f. of this channel is $\frac{K(K-1)}{K(K-1)+1}$ as stated in the following theorem.

Theorem 6 *The sum secure d.o.f. of the K-user Gaussian multiple access wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$ with probability one.*

9.1 Converse

We start with the sum rate and derive an upper bound similar to Lemma 1

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &= \sum_{i=1}^{K} H(W_i) = H(W_1^K) && (201)\\
&\leq I(W_1^K; \mathbf{Y}_1, \mathbf{Y}_2) - I(W_1^K; \mathbf{Y}_2) + nc_{15} && (202)\\
&= I(W_1^K; \mathbf{Y}_1|\mathbf{Y}_2) + nc_{15} && (203)\\
&\leq I(\mathbf{X}_1^K; \mathbf{Y}_1|\mathbf{Y}_2) + nc_{15} && (204)\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2, \mathbf{X}_1^K) + nc_{15} && (205)\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{N}_1|\mathbf{Y}_2, \mathbf{X}_1^K) + nc_{15} && (206)\\
&\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_{16} && (207)\\
&= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{17} && (208)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K|\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{17} && (209)
\end{aligned}
$$

where $W_1^K \stackrel{\triangle}{=} \{W_j\}_{j=1}^K$ and, for each j, $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$. Here $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence and $\tilde{N}_j$ is a Gaussian noise with variance $\sigma_j^2 < \min(1/h_j^2, 1/g_j^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually

independent, and are independent of all other random variables. Thus,

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K | \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{17} && (210)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K | \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_K) \\
&\quad - h(\mathbf{Y}_2) + nc_{17} && (211)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_K | \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_K) \\
&\quad - h(\mathbf{Y}_2) + nc_{17} && (212)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{18} && (213)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) + h(\mathbf{Y}_1, \mathbf{Y}_2 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) - h(\mathbf{Y}_2) + nc_{18} && (214)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) - h(\mathbf{Y}_2) + nc_{19} && (215)\\
&= \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_2) + nc_{20} && (216)\\
&\leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_{21} && (217)
\end{aligned}
$$

where (215) follows similar to (53), and (217) is due to

$$h(\tilde{\mathbf{X}}_1) \leq h(g_1\mathbf{X}_1 + \mathbf{N}_2) + nc_{22} \leq h(\mathbf{Y}_2) + nc_{22} \tag{218}$$

which is similar to going from (32) to (33) in Lemma 1 by using derivations in (60)-(65).

On the other hand, for each j, we have a bound similar to Lemma 2

$$
\begin{aligned}
\sum_{i\neq j} H(W_i) &= H(W_{\neq j}) && (219)\\
&\leq I(W_{\neq j}; \mathbf{Y}_1) + nc_{23} && (220)\\
&\leq I\left(\sum_{i\neq j} h_i\mathbf{X}_i; \mathbf{Y}_1\right) + nc_{23} && (221)\\
&= h\left(\mathbf{Y}_1\right) - h\left(\mathbf{Y}_1 \middle| \sum_{i\neq j} h_i\mathbf{X}_i\right) + nc_{23} && (222)\\
&= h\left(\mathbf{Y}_1\right) - h\left(h_j\mathbf{X}_j + \mathbf{N}_1\right) + nc_{23} && (223)\\
&\leq h(\mathbf{Y}_1) - h(\tilde{\mathbf{X}}_j) + nc_{24} && (224)
\end{aligned}
$$

where $W_{\neq j} \triangleq \{W_i\}_{i=1}^{K} \backslash \{W_j\}$ which forms the Markov chain $W_{\neq j} \to \mathbf{X}_{\neq j} \to \sum_{i\neq j} h_i\mathbf{X}_i \to$

$\mathbf{Y}_1$. Therefore, for each j, we have

$$h(\tilde{\mathbf{X}}_j) \leq h(\mathbf{Y}_1) - \sum_{i \neq j} H(W_i) + nc_{24} \tag{225}$$

Now, continuing from (217) and incorporating (225), we have

$$n \sum_{i=1}^{K} R_i \leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_{25} \tag{226}$$

$$\leq \sum_{j=2}^{K} \left[h(\mathbf{Y}_1) - \sum_{i \neq j} H(W_i) \right] + nc_{26} \tag{227}$$

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

$$nR_1 + (K-1) \sum_{j=1}^{K} nR_j \leq (K-1) h(\mathbf{Y}_1) + nc_{26} \tag{228}$$

We then apply this upper bound for each i by eliminating a different $h(\tilde{\mathbf{X}}_i)$ each time in the same way that it was done for $h(\tilde{\mathbf{X}}_1)$ in (218) and have K upper bounds in total:

$$nR_i + (K-1) \sum_{j=1}^{K} nR_j \leq (K-1) h(\mathbf{Y}_1) + nc_{26}, \qquad i = 1, 2, \cdots, K \tag{229}$$

Thus,

$$\Big[K(K-1) + 1 \Big] \sum_{j=1}^{K} nR_j \leq K(K-1) h(\mathbf{Y}_1) + nc_{27} \tag{230}$$

$$\leq K(K-1) \left(\frac{n}{2} \log P \right) + nc_{28} \tag{231}$$

that is,

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \tag{232}$$

which concludes the converse part of the theorem.

9.2 Achievable Scheme

In the Gaussian wiretap channel with M helpers, our achievability scheme divided the message signal into M parts, and each one of the M helpers protected a part at the eavesdropper. On the other hand, in the interference channel with confidential messages, since each user had its own message to send, each transmitter sent a combination of a message and a cooperative

jamming signal. We combine these two approaches to propose the following achievability scheme in this K-user multiple access wiretap channel. Each transmitter i divides its message into $(K-1)$ mutually independent sub-signals. In addition, each transmitter i sends a cooperative jamming signal U_i. At the eavesdropper Y_2, each sub-signal indexed by (i,j), where $j \in \{1,2,\cdots,K\}\backslash\{i\}$, is *aligned* with a cooperative jamming signal U_i. At the legitimate receiver Y_1, all of the cooperative jamming signals are *aligned* in the same dimension to *occupy* as *small* a signal space as possible. This scheme is illustrated in Figure 12 for the case of $K=3$.

We use in total K^2 mutually independent random variables which are

$$V_{i,j}, \quad i,j \in \{1,2,\cdots,K\}, j \neq i \tag{233}$$

$$U_k, \quad k \in \{1,2,\cdots,K\} \tag{234}$$

Each of them is uniformly and independently drawn from the same constellation $C(a,Q)$, where a and Q will be specified later. For each $i \in \{1,2,\cdots,K\}$, we choose the input signal of transmitter i as

$$X_i = \sum_{j=1,j\neq i}^{K} \frac{g_j}{g_i h_j} V_{i,j} + \frac{1}{h_i} U_i \tag{235}$$

With these input signal selections, observations of the receivers are

$$Y_1 = \sum_{i=1}^{K} \sum_{j=1,j\neq i}^{K} \frac{g_j h_i}{g_i h_j} V_{i,j} + \left[\sum_{k=1}^{K} U_k\right] + N_1 \tag{236}$$

$$Y_2 = \left[\sum_{i=1}^{K} \sum_{j=1,j\neq i}^{K} \frac{g_j}{h_j} V_{i,j}\right] + \sum_{j=1}^{K} \frac{g_j}{h_j} U_j + N_2 \tag{237}$$

$$= \sum_{j=1}^{K} \frac{g_j}{h_j} \left[U_j + \sum_{i=1,i\neq j}^{K} V_{i,j}\right] + N_2 \tag{238}$$

By [29, Theorem 1], we can achieve the following sum secrecy rate

$$\sup \sum_{i=1}^{K} R_i \geq I(\mathbf{V};Y_1) - I(\mathbf{V};Y_2) \tag{239}$$

where $\mathbf{V} \triangleq \{V_{i,j} : i,j \in \{1,2,\cdots,K\}, j \neq i\}$.

Now, we first bound the probability of decoding error. Note that the *space* observed at receiver 1 consists of $(2Q+1)^{K(K-1)}(2KQ+1)$ points in $K(K-1)+1$ *dimensions*, and the sub-signal in each *dimension* is drawn from a constellation of $C(a,KQ)$. Here, we use the property that $C(a,Q) \subset C(a,KQ)$. By using Khintchine-Groshev theorem of Diophantine approximation in number theory, we can bound the minimum distance d_{min} between the

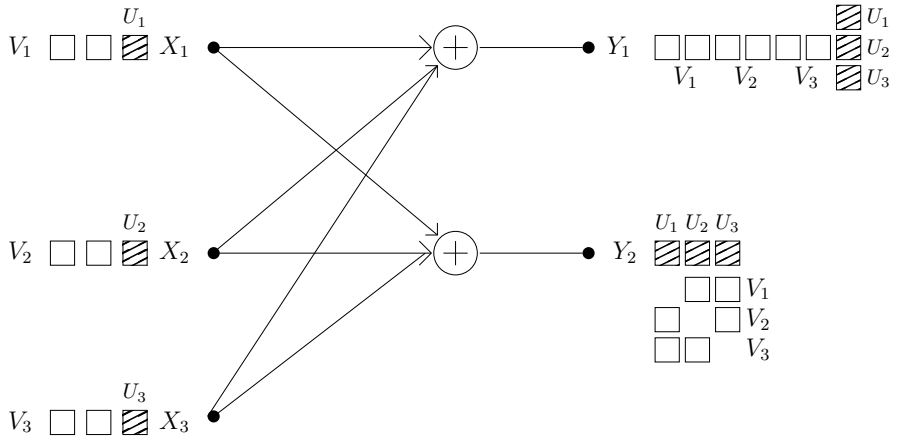

Figure 12: Illustration of interference alignment for the K-user multiple access wiretap channel. Here, $K = 3$.

points in the receiver's *space*, i.e., for any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{(KQ)^{K(K-1)+\delta}} \tag{240}$$

for almost all rationally independent factors in the Y_1 except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as,

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(KQ)^{2(K(K-1)+\delta)}}\right) \tag{241}$$

where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(K(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P, then

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P}{8(KQ)^{2(K(K-1)+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+\delta)}}\right) \tag{242}$$

and we can have $\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose

$$\gamma \leq \min_i \frac{1}{\sqrt{\sum_{j=1, j\neq i}^{K} \left(\frac{g_j}{g_i h_j}\right)^2 + \left(\frac{1}{h_i}\right)^2}} \tag{243}$$

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

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{244}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+1+\delta)}}\right) \log(2Q+1)^{K(K-1)} \tag{245}$$

which means that

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{246}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+1+\delta)}}\right)\right] \log(2Q+1)^{K(K-1)} - 1 \tag{247}$$

On the other hand,

$$I(\mathbf{V}; Y_2) \leq I\left(\mathbf{V}; \sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) \tag{248}$$

$$= H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right] \middle| \mathbf{V}\right) \tag{249}$$

$$= H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K} \frac{g_j}{h_j} U_j\right) \tag{250}$$

$$\leq K \log \frac{2KQ+1}{2Q+1} \tag{251}$$

$$\leq K \log K \tag{252}$$

where (250) is due to the fact that entropy is maximized by the uniform distribution which takes values over a set of cardinality $(2KQ+1)^K$.

Combining (247) and (252), we obtain

$$\sup \sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{253}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+1+\delta)}}\right)\right] \log(2Q+1)^{K(K-1)} - 1 - K \log K \tag{254}$$

$$= \frac{K(K-1)(1-\delta)}{K(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{255}$$

where $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{K(K-1)}{K(K-1)+1}$ sum secure d.o.f. with probability one.

10 Conclusion

We determined the secure d.o.f. of several fundamental channel models in one-hop wireless networks. We first considered the Gaussian wiretap channel with one helper. While the helper needs to create interference at the eavesdropper, it should not create too much interference at the legitimate receiver. Our approach is based on understanding this trade-off that the helper needs to strike. To that purpose, we developed an upper bound that relates the entropy of the cooperative jamming signal from the helper and the message rate. In addition, we developed an achievable scheme based on real interference alignment which aligns the cooperative jamming signal from the helper in the same *dimension* as the message signal. This ensures that the information leakage rate is upper bounded by a constant which does not scale with the power. In addition, to help the legitimate user decode the message, our achievable scheme renders the message signal and the cooperative jamming signal distinguishable at the legitimate receiver. This essentially implies that the message signal can *occupy* only half of the available space in terms of the degrees of freedom. Consequently, we showed that the exact secure d.o.f. of the Gaussian wiretap channel with one helper is $\frac{1}{2}$ by these matching achieavibility and converse proofs. We then generalized our achievability and converse techniques to the Gaussian wiretap channel with M helpers, Gaussian broadcast channel with confidential messages and helpers, two-user Gaussian interference channel with confidential messages and helpers, and K-user Gaussian multiple access wiretap channel. In the multiple-message settings, transmitters needed to send a mix of their own messages and cooperative jamming signals. We determined the exact secure d.o.f. in all of these system models.

A An Alternative Proof for the Multiplexing Gain of the K-User Gaussian Interference Channel

The original proof for this setting is given by [37]. Here, we provide an alternative proof for the $K = 2$ case by using Lemma 2, and then extend it to the case of general K.

For $K = 2$, the channel model for the two-user Gaussian interference channel is

$$Y_1 = h_{1,1}X_1 + h_{2,1}X_2 + N_1 \tag{256}$$

$$Y_2 = h_{1,2}X_1 + h_{2,2}X_2 + N_2 \tag{257}$$

We start with the definition of the sum rate

$$\begin{aligned}
nR_1 + nR_2 &= H(W_1, W_2) && (258)\\
&= H(W_1, W_2|\mathbf{Y}_1, \mathbf{Y}_2) + I(W_1, W_2; \mathbf{Y}_1, \mathbf{Y}_2) && (259)\\
&\leq I(W_1, W_2; \mathbf{Y}_1, \mathbf{Y}_2) + nc_{29} && (260)\\
&= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_1, \mathbf{Y}_2|W_1, W_2) + nc_{29} && (261)\\
&\leq h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_1, \mathbf{Y}_2|\mathbf{X}_1, \mathbf{X}_2, W_1, W_2) + nc_{29} && (262)\\
&\leq h(\mathbf{Y}_1, \mathbf{Y}_2) + nc_{30} && (263)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2|\mathbf{Y}_1, \mathbf{Y}_2) + nc_{30} && (264)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2) + nc_{30} && (265)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) + nc_{31} && (266)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{31} && (267)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{32} && (268)
\end{aligned}$$

where the last inequality follows similar to (53) after a derivation similar to (55)-(59), and, for each j, $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$. Here $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$, which is Gaussian with variance $\sigma_j^2 < \min(1/h_{j,1}^2, 1/h_{j,2}^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables.

Then, we apply Lemma 2 to characterize the interference from X_1 to transmitter-receiver pair 2 and from X_2 to transmitter-receiver pair 1

$$\begin{aligned}
nR_1 + nR_2 &\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{32} && (269)\\
&\leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + nc_{32} && (270)\\
&\leq h(\mathbf{Y}_2) - H(W_2) + h(\mathbf{Y}_1) - H(W_1) + nc_{33} && (271)
\end{aligned}$$

By noting that $H(W_1) = nR_1$ and $H(W_2) = nR_2$, we have

$$\begin{aligned}
2(nR_1 + nR_2) &\leq h(\mathbf{Y}_2) + h(\mathbf{Y}_1) + nc_{33} && (272)\\
&\leq 2\left(\frac{n}{2}\log P\right) + nc_{34} && (273)
\end{aligned}$$

which implies that

$$D_\Sigma \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \leq 1 \qquad (274)$$

i.e., the multiplexing gain of the two-user Gaussian interference channel is not greater than 1. By the argument in [37, Proposition 1], we can conclude that the multiplexing gain of the K-user Gaussian interference channel is at most $\frac{K}{2}$.

References

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

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

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

[4] 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.

[5] 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.

[6] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, June 2008.

[7] 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.

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

[10] 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.

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

[12] 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.

[13] 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.

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

[15] 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.

[16] 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].

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

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

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

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

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

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.

[27] 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].

[28] X. He. *Cooperation and information theoretic security in wireless networks.* Ph.D. dissertation, Pennsylvania State University, Pennsylvania, 2010.

[29] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure Degrees-of-Freedom of the multiple-access-channel. *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729].

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

[31] 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.

[32] 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.

[33] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. In *IEEE Global Telecommunications Conference*, Honolulu, Hawaii, December 2009.

[34] 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].

[35] 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].

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

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

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