Secure Degrees of Freedom of the Gaussian Wiretap Channel with Helpers

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

Abstract— **The 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 $\frac{M}{M+1}$.**

I. Introduction

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]. 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 determine the exact secure d.o.f. of the Gaussian wiretap channel with M helpers by characterizing this trade-off in the cooperative jamming signals of the helpers.

We start by considering the Gaussian wiretap channel with a single helper, as shown in Fig. 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] 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

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

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 Fig. 3). 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] 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 develop a relationship between the cooperative jamming signal from the independent helper and the message rate. Since 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, 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 Fig. 4). 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.

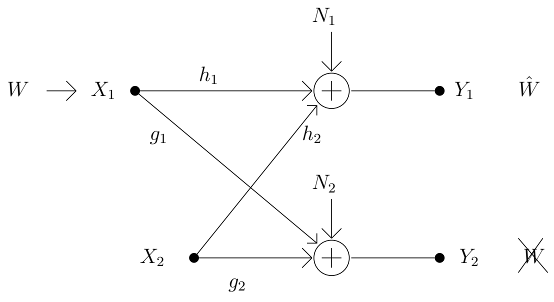

Fig. 1. Gaussian wiretap channel with one helper.

II. System Model and Definitions

The Gaussian wiretap channel with helpers (see Fig. 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 gains are time-invariant, and independently drawn from continuous distributions. 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 $R \overset{\triangle}{=} \frac{1}{n} \log |\mathcal{W}|$, 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 $\mathbf{X}_1 \stackrel{\triangle}{=} X_1^n$ is the n-length channel input.[1] 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, 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

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

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, we assume that $M \geq 1$ and $h_j \neq 0$ and $g_j \neq 0$ for all $j = 1, \cdots, M+1$.

III. General Converse Results

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

A. Secrecy Penalty

In the following lemma, we give a general upper bound for the secrecy rate between transmitter 1 and receiver 1 by working with n-letter signals. 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 (7). 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 (8).

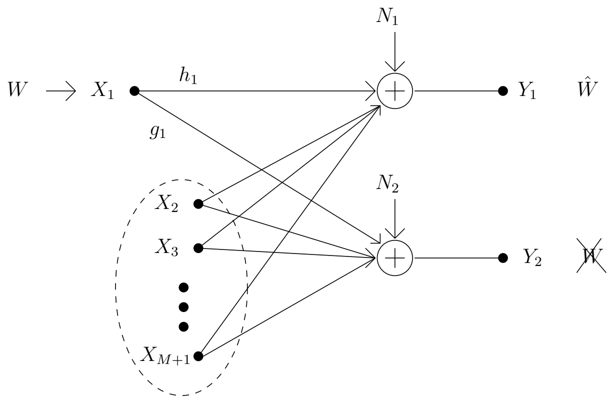

Fig. 2. Gaussian wiretap channel with M helpers.

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

$$nR \leq \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc \tag{7}$$

$$\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{8}$$

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:

$$\begin{aligned} nR &= H(W) = H(W|\mathbf{Y}_1) + I(W; \mathbf{Y}_1) && (9)\\ &\leq I(W; \mathbf{Y}_1) + nc_1 && (10)\\ &\leq I(W; \mathbf{Y}_1) - I(W; \mathbf{Y}_2) + nc_2 && (11) \end{aligned}$$

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

$$\begin{aligned} nR &\leq I(W; \mathbf{Y}_1, \mathbf{Y}_2) - I(W; \mathbf{Y}_2) + nc_2 && (12)\\ &= I(W; \mathbf{Y}_1|\mathbf{Y}_2) + nc_2 && (13)\\ &= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2, W) + nc_2 && (14)\\ &\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && (15) \end{aligned}$$

where (15) is due to

$$\begin{aligned} h(\mathbf{Y}_1|\mathbf{Y}_2, W) &\geq h(\mathbf{Y}_1|\mathbf{X}_1, \cdots, \mathbf{X}_{M+1}, \mathbf{Y}_2, W) && (16)\\ &= h(\mathbf{N}_1|\mathbf{X}_1, \cdots, \mathbf{X}_{M+1}, \mathbf{Y}_2, W) && (17)\\ &= h(\mathbf{N}_1) && (18)\\ &= \frac{n}{2}\log 2\pi e && (19) \end{aligned}$$

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

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 (15),

$$\begin{aligned}
nR &\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && (20)\\
&= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (21)\\
&= h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2)\\
&\quad - h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (22)\\
&\leq h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2)\\
&\quad - h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \cdots, \mathbf{X}_{M+1})\\
&\quad - h(\mathbf{Y}_2) + nc_3 && (23)\\
&\leq h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2)\\
&\quad - h(\tilde{\mathbf{N}}_1, \cdots, \tilde{\mathbf{N}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \cdots, \mathbf{X}_{M+1})\\
&\quad - h(\mathbf{Y}_2) + nc_3 && (24)\\
&\leq h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2)\\
&\quad - h(\tilde{\mathbf{N}}_1, \cdots, \tilde{\mathbf{N}}_{M+1}) - h(\mathbf{Y}_2) + nc_3 && (25)\\
&\leq h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_4 && (26)\\
&= h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1})\\
&\quad + h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_4 && (27)\\
&\leq h(\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_5 && (28)\\
&= \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc_5 && (29)
\end{aligned}$$

where (28) is due to $h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}) \leq nc_6$. 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

$$\begin{aligned}
&h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1})\\
&\quad\leq h(\mathbf{Y}_1|\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}) + h(\mathbf{Y}_2|\tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}) && (30)\\
&\quad= h\left(\sum_{i=1}^{M+1} h_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}\right)\\
&\qquad + h\left(\sum_{i=1}^{M+1} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}\right) && (31)\\
&\quad= h\left(-\sum_{i=1}^{M+1} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}\right)\\
&\qquad + h\left(-\sum_{i=1}^{M+1} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \cdots, \tilde{\mathbf{X}}_{M+1}\right) && (32)\\
&\quad\leq h\left(-\sum_{i=1}^{M+1} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1\right) + h\left(-\sum_{i=1}^{M+1} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2\right) && (33)\\
&\quad\stackrel{\triangle}{=} nc_6 && (34)
\end{aligned}$$

which completes the proof of (7).

Finally, we show (8). 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.,

$$\mathbf{Y}_2 = g_j\mathbf{X}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}_2 \tag{35}$$

$$\tilde{\mathbf{Y}}_2 = g_j\tilde{\mathbf{X}}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}'_2 \tag{36}$$

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

$$\begin{aligned}
h(\mathbf{Y}_2) &= h(\tilde{\mathbf{Y}}_2) && (37)\\
&= h\left(g_j\tilde{\mathbf{X}}_j + \sum_{i=1, i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}'_2\right) && (38)\\
&\geq h\left(g_j\tilde{\mathbf{X}}_j\right) && (39)\\
&= n\log|g_j| + h(\tilde{\mathbf{X}}_j) && (40)
\end{aligned}$$

where (39) is due to the differential entropy version of [37, Problem 2.14]. Substituting this into (7) gives us (8). ■

B. 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 (41), 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, (41), 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.

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

$$h(\mathbf{X}_j + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_1) - H(W) + nc \tag{41}$$

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

$$\begin{aligned} nR = H(W) &\le I(\mathbf{X}_1;\mathbf{Y}_1) && (42)\\ &= h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\mathbf{X}_1) && (43)\\ &= h(\mathbf{Y}_1) - h\left(\sum_{i=2}^{M+1} h_i\mathbf{X}_i + \mathbf{N}_1\right) && (44)\\ &\le h(\mathbf{Y}_1) - h\left(h_j\mathbf{X}_j + \mathbf{N}_1\right) && (45)\\ &\le h(\mathbf{Y}_1) - h\left(h_j\mathbf{X}_j + h_j\tilde{\mathbf{N}}\right) && (46)\\ &= h(\mathbf{Y}_1) - h\left(\mathbf{X}_j + \tilde{\mathbf{N}}\right) + nc && (47) \end{aligned}$$

where (45) and (46) are due to the differential entropy version of [37, Problem 2.14]. In going from (45) to (46), 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. ■

IV. Wiretap Channel with One Helper

In this section, we consider the Gaussian wiretap channel with one helper and show that the secure d.o.f. is $\frac{1}{2}$ for almost all channel gains as stated in the following theorem.

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

A. Converse

We start with (8) of Lemma 1 with $M = 1$ and by choosing $j = 1$,

$$\begin{aligned} nR &\le \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' && (48)\\ &= h(\tilde{\mathbf{X}}_2) + nc' && (49)\\ &\le h(\mathbf{Y}_1) - H(W) + nc_7 && (50)\\ &\le \frac{n}{2}\log P - H(W) + nc_8 && (51) \end{aligned}$$

where (50) is due to Lemma 2. By noting $H(W) = nR$ and using (5), (51) implies that

$$D_s \le \frac{1}{2} \qquad (52)$$

which concludes the converse part of the theorem.

B. Achievable Scheme

To show the achievability by interference alignment, we slightly change the notation. Let $\bar{X}_1 \triangleq g_1X_1$, $\bar{X}_2 \triangleq g_2X_2$, $\alpha \triangleq h_1/g_1$, and $\beta \triangleq h_2/g_2$. Then, the channel model becomes

$$\begin{aligned} Y_1 &= \alpha\bar{X}_1 + \beta\bar{X}_2 + N_1 && (53)\\ Y_2 &= \bar{X}_1 + \bar{X}_2 + N_2 && (54) \end{aligned}$$

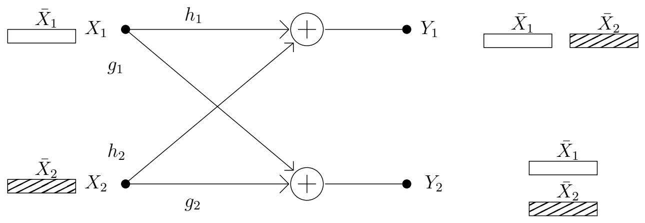

Fig. 3. Illustration of interference alignment for the Gaussian wiretap channel with one helper.

Here $\bar{X}_1$ is the input signal carrying 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 Fig. 3, 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

$$C(a,Q) = a\{-Q, -Q+1, \dots, Q-1, Q\} \qquad (55)$$

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 [2]

$$C_s \ge I(\bar{X}_1;Y_1) - I(\bar{X}_1;Y_2) \qquad (56)$$

In order to show that $D_s \ge \frac{1}{2}$, 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

$$H(\bar{X}_1) = H(\bar{X}_2) = \log|C(a,Q)| = \log(2Q+1) \qquad (57)$$

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.,

$$Y_1 - N_1 = \alpha\bar{X}_1 + \beta\bar{X}_2 \qquad (58)$$

where α and β are rationally independent real numbers[2] with probability 1.

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 $\delta > 0$,

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

there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{Q^{1+\delta}} \tag{59}$$

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,

$$\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8Q^{2(1+\delta)}}\right) \tag{60}$$

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

$$\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 P}{8Q^{2(1+\delta)+2}}\right) = \exp\left(-\frac{k_\delta^2 \gamma^2 P^\delta}{8}\right) \tag{61}$$

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

$$\begin{aligned} H(\bar{X}_1|Y_1) &\leq H(\bar{X}_1|\hat{X}_1) & (62)\\ &\leq 1 + \exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{8}\right)\log(2Q+1) & (63)\end{aligned}$$

which means that

$$\begin{aligned} I(\bar{X}_1; Y_1) &= H(\bar{X}_1) - H(\bar{X}_1|Y_1) & (64)\\ &\geq \left[1 - \exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{8}\right)\right]\log(2Q+1) - 1 & (65)\end{aligned}$$

On the other hand,

$$\begin{aligned} I(\bar{X}_1; Y_2) &\leq I(\bar{X}_1; \bar{X}_1 + \bar{X}_2) & (66)\\ &= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2|\bar{X}_1) & (67)\\ &= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2) & (68)\\ &\leq \log(4Q+1) - \log(2Q+1) & (69)\\ &\leq \log\frac{4Q+1}{2Q+1} & (70)\\ &\leq 1 & (71)\end{aligned}$$

where (69) 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 (65) and (71), we have

$$\begin{aligned} C_s &\geq I(\bar{X}_1; Y_1) - I(\bar{X}_1; Y_2) & (72)\\ &\geq \left[1 - \exp\left(-\frac{k_\delta^2\gamma^2 P^\delta}{8}\right)\right]\log(2Q+1) - 2 & (73)\\ &= \frac{1-\delta}{(2+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) & (74)\end{aligned}$$

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.

V. Wiretap Channel with M Helpers

In this section, we consider the Gaussian wiretap channel with M helpers and 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.

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

A. Converse

We again start with (8) of Lemma 1 with the selection of $j = 1$

$$\begin{aligned} nR &\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' & (75)\\ &= \sum_{i=2}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' & (76)\\ &\leq M[h(\mathbf{Y}_1) - H(W)] + nc_9 & (77)\end{aligned}$$

where (77) is due to Lemma 2 for each jamming signal $\tilde{\mathbf{X}}_i$, $i = 2, 3, \cdots, M+1$. By noting $H(W) = nR$, (77) implies

$$\begin{aligned} (M+1)nR &\leq Mh(\mathbf{Y}_1) + nc_9 & (78)\\ &\leq M\left(\frac{n}{2}\log P\right) + nc_{10} & (79)\end{aligned}$$

which further implies from (5) that

$$D_s \leq \frac{M}{M+1} \tag{80}$$

which concludes the converse part of the theorem.

B. 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

$$X_1 = \sum_{k=2}^{M+1} \frac{g_k}{g_1 h_k} V_k \tag{81}$$

and the input signal of the jth helper as

$$X_j = \frac{1}{h_j} U_j, \quad j = 2, 3, \cdots, M+1 \tag{82}$$

Then, the observations of the receivers are

$$Y_1 = \sum_{k=2}^{M+1} \frac{h_1 g_k}{g_1 h_k} V_k + \left(\sum_{j=2}^{M+1} U_j\right) + N_1 \tag{83}$$

$$Y_2 = \sum_{k=2}^{M+1} \frac{g_k}{h_k}\Big(V_k + U_k\Big) + N_2 \tag{84}$$

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 Fig. 4.

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 [2]

$$C_s \geq I(X_1; Y_1) - I(X_1; Y_2) \tag{85}$$

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

$$d_{min} \geq \frac{k_\delta a}{(MQ)^{M+\delta}} \tag{86}$$

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,

$$\Pr\left[X_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \leq \exp\left(-\frac{a^2 k_\delta^2}{8(MQ)^{2(M+\delta)}}\right) \tag{87}$$

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 constant independent of P, then

$$\Pr\left[X_1 \neq \hat{X}_1\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P}{8(MQ)^{2(M+\delta)+2}}\right) \tag{88}$$

$$= \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right) \tag{89}$$

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

$$\gamma \leq \min([\sum_{k=2}^{M+1}(\frac{g_k}{g_1 h_k})^2]^{-1/2}, |h_2|, |h_3|, \cdots, |h_{M+1}|) \tag{90}$$

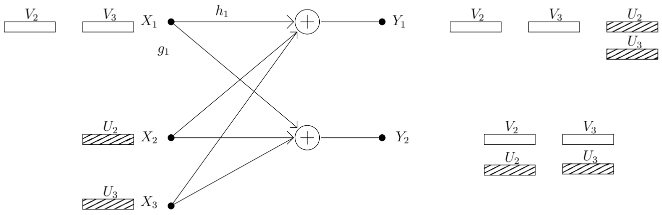

Fig. 4. Illustration of interference alignment for the Gaussian wiretap channel with M helpers. Here, $M = 2$.

By Fano's inequality and the Markov chain $X_1 \to Y_1 \to \hat{X}_1$, we know that

$$H(X_1|Y_1) \leq H(X_1|\hat{X}_1) \tag{91}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right) \log(2Q+1)^M \tag{92}$$

which means that

$$I(X_1; Y_1) = H(X_1) - H(X_1|Y_1) \tag{93}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right)\right] \log(2Q+1)^M - 1 \tag{94}$$

On the other hand,

$$I(X_1; Y_2) \leq I\left(X_1; \sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) \tag{95}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\Big| X_1\right) \tag{96}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}U_k\right) \tag{97}$$

$$\leq \log(4Q+1)^M - \log(2Q+1)^M \tag{98}$$

$$\leq M \log\frac{4Q+1}{2Q+1} \tag{99}$$

$$\leq M \tag{100}$$

where (98) 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 (94) and (100), we have

$$C_s \geq I(X_1; Y_1) - I(X_1; Y_2) \tag{101}$$

$$\geq \left[1 - \exp\left(-\frac{k_\delta^2 \gamma^2 M^2 P^\delta}{8M^{2(M+1+\delta)}}\right)\right] \log(2Q+1)^M - (M+1) \tag{102}$$

$$= \frac{M(1-\delta)}{(M+1+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{103}$$

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.

VI. Conclusion

We determined the secure d.o.f. of the Gaussian wiretap channel with helpers. 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 and cooperative jamming which aligns the cooperative jamming signal from the helper in the same *dimension* as the message signal at the eavesdropper, which in turn 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 and determined its exact secure d.o.f. as $\frac{M}{M+1}$.

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