INVITED PAPER

Secure Degrees of Freedom of Multiuser Networks: One-Time-Pads in the Air via Alignment

Interference alignment techniques are powerful methods that best exploit available degrees of freedom in multiterminal settings. Extensions involving secure degrees of freedom are reviewed in an expository manner, focusing on the secrecy penalty and role of a helper in the design of secure systems using real interference alignment, cooperative jamming, and structured signaling.

By Jianwei Xie and Sennur Ulukus, *Member IEEE*

ABSTRACT | We revisit the recent secure degrees of freedom (s.d.o.f.) results for one-hop multiuser wireless networks by considering three fundamental wireless network structures: Gaussian wiretap channel with helpers, Gaussian multiple access wiretap channel, and Gaussian interference channel with secrecy constraints. We present main enabling tools and resulting communication schemes in an expository manner, along with key insights and design principles emerging from them. The main achievable schemes are based on real interference alignment, channel prefixing via cooperative jamming, and structured signalling. Real interference alignment enables aligning the cooperative jamming signals together with the message carrying signals at the eavesdroppers to protect them akin to one-time-pad protecting messages in wired systems. Real interference alignment also enables decodability at the legitimate receivers by rendering message carrying and cooperative jamming signals separable, and simultaneously aligning the cooperative jamming signals in the smallest possible subspace. The main converse techniques are based on two key lemmas which quantify 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; and the *role of a helper* by developing a direct relationship between the cooperative jamming signal of a helper and the message rate. These two lemmas when applied according to the unique structure of individual networks provide tight converses. Finally, we present a blind cooperative jamming scheme for the helper network with no eavesdropper channel state information at the transmitters that achieves the same optimal s.d.o.f. as in the case of full eavesdropper channel state information.

KEYWORDS | Cooperative jamming; interference alignment; interference channel; multiple access channel; secure degrees of freedom; wiretap channel

I. INTRODUCTION

We consider several fundamental multiuser network structures under secrecy constraints: Gaussian wiretap channel with M helpers, K-user Gaussian multiple access wiretap channel and K-user Gaussian interference channel with secrecy constraints. Security of communication was first considered by Shannon in [1], where a legitimate pair wishes to have secure communication in the presence of an eavesdropper over a noiseless channel, leading to the necessity of secure keys and the one-time-pad encryption method, in that model. Wyner introduced the noisy wiretap channel, and demonstrated that secure communication can be attained by stochastic encoding without

Manuscript received January 29, 2015; revised May 7, 2015; accepted June 10, 2015. Date of publication August 18, 2015; date of current version September 16, 2015. This work was supported by the NSF under Grants CNS 09-64632, CCF 09-64645, CCF 10-18185, and CNS 11-47811.

J. Xie was with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. He is now with Google Inc., Mountain View, CA 94043 USA (e-mail: xiejw@google.com).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Digital Object Identifier: 10.1109/JPROC.2015.2445914

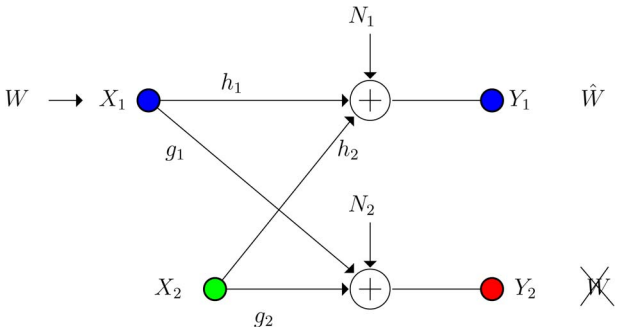


Fig. 1. *Gaussian wiretap channel with one helper.*

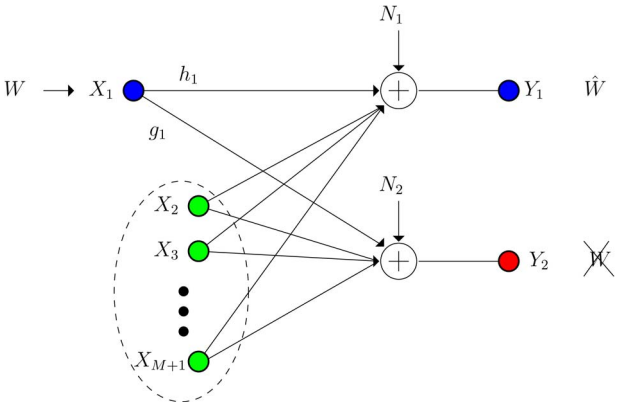


Fig. 2. *Gaussian wiretap channel with M helpers.*

using any keys, if the eavesdropper is degraded with respect to the legitimate receiver [2]. Csiszar and Korner generalized his result to arbitrary, not necessarily degraded, wiretap channels, and showed that secure communication is still possible, even when the eavesdropper is not degraded [3]. Csiszar and Korner introduced channel prefixing and rate splitting into the achievable scheme in addition to Wyner's stochastic encoding. Leung–Yan–Cheong and Hellman obtained the capacity-equivocation region of the Gaussian wiretap channel [4], which is degraded.

This line of research has been subsequently extended to many multiuser settings, e.g., broadcast channels with confidential messages [5]–[10], multireceiver wiretap channels [11]–[15], interference channels with confidential messages and/or external eavesdroppers [5], [16]–[18], multiple access wiretap channels [19]–[23], relay eavesdropper channels [24]–[27], untrusted relay channels [28], [29], two-way wiretap channels [20], [30]–[32], multiway relay wiretap channels [33], compound wiretap channels [34], [35], etc. For many of these networks, even in simple Gaussian settings, exact secrecy capacity regions are still unknown. Here, we focus on Gaussian wiretap channel with helpers, Gaussian multiple access wiretap channel and Gaussian interference channel with secrecy constraints, for all of which, the exact secrecy capacity regions are unknown. In the absence of exact secrecy capacity regions, achievable secure degrees of freedom (s.d.o.f.) at high signal-to-noise ratio (SNR) regimes has been studied in the literature [36]–[58]. In this paper, we revisit the results, insights, and main tools presented in a sequence of papers in [46]–[54], which determined the exact s.d.o.f. regions of all of these three classes of networks.

In the canonical Gaussian wiretap channel, Gaussian signalling is optimal, and the secrecy capacity is the difference of the channel capacities of the transmitter-receiver and the transmitter-eavesdropper pairs [4]. It is well-known that this difference does not scale with the SNR, and hence the s.d.o.f. of the Gaussian wiretap channel is zero, indicating a severe penalty due to secrecy in this case. If there is a helper in the system, as shown in Fig. 1, the helper can improve the achievable secrecy rate of the main transmitter by sending cooperative jamming signals [19], [20]. The secrecy capacity of a wiretap channel with a helper, and the optimal helping strategy are unknown. However, it is known that the s.d.o.f. of this system with independent identically distributed (i.i.d.) Gaussian cooperative jamming signals is still zero [42], [59]. In addition, in earlier work, it is observed that strictly positive s.d.o.f. can be obtained, for instance, by using structured codes [39], [40] or by using non-i.i.d. Gaussian signalling [42]. References [46] and [48] determined the exact optimal s.d.o.f. of a wiretap channel with an arbitrary number of (M) helpers, see Fig. 2, and also the optimal helper signalling in the sense of achieving the largest s.d.o.f. The emerging idea in [46], [48] for optimal s.d.o.f. is that the cooperation signals should not have too much randomness (hence the suboptimality of i.i.d. Gaussian signalling), as they hurt both the legitimate receiver and the eavesdropper. Therefore, *weaker* cooperative jamming signals are needed, and that the received subspaces at the legitimate receiver and the eavesdropper need to be carefully controlled.

The achievable scheme in [46] and [48] is based on real interference alignment [60], [61] and cooperative jamming [20], and is as follows: The legitimate receiver divides its message into M parts, where M is the number of helpers. Each one of M helpers sends a cooperative jamming signal. All signals, both message carrying and cooperative jamming signals, come from structured pulse amplitude modulation (PAM) constellations. Each one of the cooperative jamming signals is aligned with a message carrying signal at the eavesdropper; see Fig. 5. This action protects the message by limiting the information leakage to the eavesdropper. This is akin to *one-time-pad* in wired systems [1]. In one-time-pad, when a uniformly distributed message signal W is XORed with an independent and uniformly distributed key K, the overall signal $X = W \oplus K$ becomes statistically independent of the message, i.e., $I(X;W) = 0$, i.e., information leakage to the eavesdropper is exactly zero. With real interference alignment and uniform PAM signals, we show that the

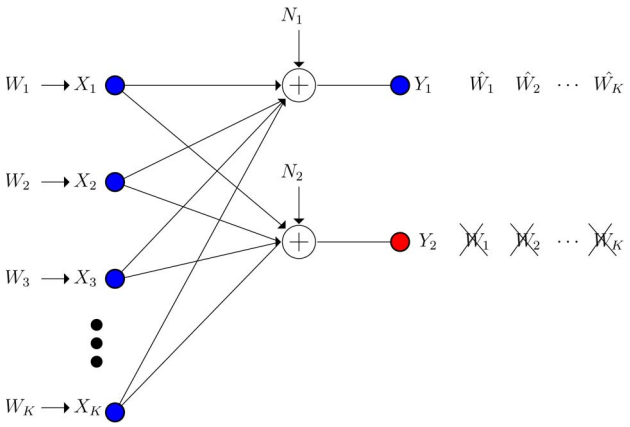


Fig. 3. *K-user multiple access wiretap channel.*

mutual information between the messages and the eavesdropper's observation is not exactly zero, but is upper bounded by a constant, and therefore, is effectively zero in terms of s.d.o.f. At the same time, all of the cooperative jamming signals are aligned in the smallest subspace at the legitimate receiver, and are separated from the message carrying signals, see Fig. 5, in order to allow for the largest subspace for the useful signals and enable their decodability. The details of the performance analysis in terms of rate and equivocation achieved by this scheme is based on the Khintchine–Groshev theorem of Diophantine approximation in number theory.

The converse developed in [46] and [48] for this channel model has two key steps. First, the secrecy rate is upper bounded by the difference of the sum of differential entropies of the channel inputs of the legitimate receiver and the helpers and the differential entropy of the eavesdropper's observation. Due to the eavesdropper's observation, one of the independent channel inputs is eliminated, and that is why this fact is named the *secrecy penalty* lemma. In the second step, a direct relationship is developed between the cooperative jamming signal from an independent helper and the message rate. The motivation of this step, which is named, *role of a helper* lemma, is to determine the optimum action (role) of a helper: 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. This lemma identifies this constraint by developing an upper bound on the differential entropy of the cooperative jamming signal coming from a helper in terms of the message rate. By using these two lemmas, and the achievable scheme described above, [46], [48] determine the exact s.d.o.f. of the Gaussian wiretap channel with M helpers to be $M/(M+1)$.

For the case of K-user multiple access wiretap channel, see Fig. 3, where all K users have messages to be hidden from an external eavesdropper, [47], [48] show that, the exact sum s.d.o.f. is $K(K-1)/(K(K-1)+1)$. Note that this is larger than one user utilizing the remaining $K-1$ users as helpers, which gives a s.d.o.f. of $(K-1)/K$, and time-sharing between such strategies among all users. Therefore, the fact that all users in the system have messages enables the system as a whole to obtain a higher sum s.d.o.f. The converse in this case is by extending the *secrecy penalty* and *role of a helper* lemmas to a multimessage setting. The achievability is by real interference alignment, channel prefixing by cooperative jamming, and structured signalling. Specifically, each transmitter divides its message into $K-1$ submessages, and sends these messages together with a cooperative jamming signal; see Fig. 6. All of the signals come from the same structured PAM constellation. Each cooperative jamming signal is aligned with $K-1$ message carrying signals at the eavesdropper, protecting all of them simultaneously. At the same time, all of the K cooperative jamming signals are aligned in the smallest subspace at the legitimate receiver. Different from the helper setting, here all transmitters send a mix of message carrying signals and cooperative jamming signals. This is an instance of *channel prefixing* [3] where the actual channel input is a further randomization of the message carrying signal.

For the case of K-user interference channel with secrecy constraints, [49], [50] consider the cases of *confidential messages* where each transmitter's message is to be kept secret from the $K-1$ legitimate receivers, *external eavesdropper* where all transmitters' messages are to be kept secret from an external eavesdropper, and the combination of the two where all messages are to be kept secret from K receivers one of which is the external eavesdropper, and show that, for all of these three cases, the exact sum s.d.o.f. is $K(K-1)/(2K-1)$. Since each message is needed to be kept secret from multiple receivers, the bounding techniques in [48] are extended in [49] and [50] to be valid for the interference channel setting, by focusing on the eavesdroppers as opposed to the messages, and then by sequentially applying the *role of a helper* lemma to each transmitter by treating its signal as a helper to another specific transmitter. For achievability, for the $K=2$ user interference channel with confidential messages case, since each message needs to be aligned at only two receivers, [48] develops a real alignment and cooperative jamming based scheme as in the cases of helper and multiple access networks. However, for the general K-user case, each message needs to be delivered to a receiver and protected from K other receivers, which requires careful simultaneous alignment at $K+1$ receivers. References [49] and [50] achieve this alignment by using an *asymptotical* real interference alignment technique [61], where many signals are introduced to carry each message, and they are aligned simultaneously at multiple receivers *only order-wise* (i.e., we align most of them, but not all of them), and by developing a method to

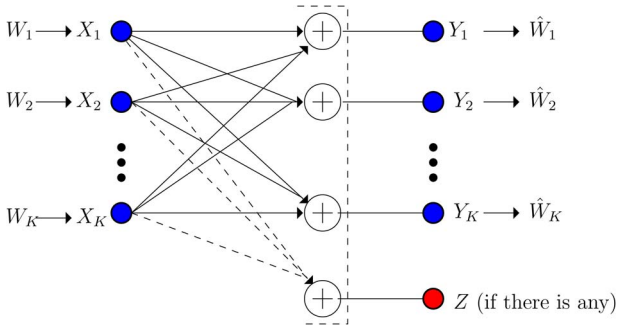


Fig. 4. *K-user Gaussian interference channel with secrecy constraints.*

upper bound the information leakage rate by a function which can be made small.

While [47]–[50] determine the *sum* s.d.o.f. of multiple access and interference channels with secrecy constraints, references [51]–[53] establish the entire s.d.o.f. *regions*. Such regions show the trade-offs between the achievable s.d.o.f. of individual users. In order to determine the s.d.o.f. regions, asymmetric (not only *sum*) s.d.o.f. expressions are developed. In addition, in the case of interference channels, constraints due to interference also, in addition to secrecy, are needed in the final region expressions. For achievability, [51]–[53] observe that the converse regions have a *polytope* structure, and develop achievable schemes that achieve the extreme points of the polytope region. The major effort in [51]–[53] is to efficiently enumerate all of the extreme points of the converse region, and then to develop an achievable scheme for each extreme point of this region; the achievability of the entire region then follows from time-sharing.

A crucial property of all of the scenarios considered so far is that the transmitters have full channel state information (CSI) of all channels in the system. In fact, these CSI are carefully utilized in the corresponding alignment schemes. Reference [54] considers a practically relevant scenario, where in a wiretap channel with helpers, the transmitters have CSI only to the legitimate receiver, but no CSI to the eavesdropper. Reference [54] shows the surprising result that, in this helper network, even without any eavesdropper CSI, the optimal s.d.o.f. of $M/(M+1)$ can be achieved. The converse to this result follows from the converse for the case of full CSI in [46] and [48]. The achievability is by a *blind alignment* scheme inspired by [56]. In the scheme proposed in [54], all helpers as well as the legitimate transmitter send cooperative jamming signals; see Fig. 11 and compare it with Fig. 5. In this system, there are a total of $M+1$ cooperative jamming signals which span the decoding space of the eavesdropper and hence protect the M message carrying signals. Note that, exact alignment at the eavesdropper is not possible, as eavesdropper CSI is unknown at the transmitters. In this setting, a different technique is used to prove that the information leakage to the eavesdropper is upper bounded. In addition, here, the CSI to the legitimate receiver is used to align all of the $M+1$ cooperative jamming signals in the smallest subspace at the legitimate receiver.[1]

II. MAIN TOOLS

In this section, we review main tools used in this paper. The converse tools include two lemmas: Lemma 1, which is the *secrecy penalty* lemma, and Lemma 2, which is the *role of a helper* lemma. The achievability tool is the technique of *real interference alignment*, which is stated in Lemma 3.

A. Converse Tools: Secrecy Penalty and Role of a Helper Lemmas

In the following lemma (Lemma 1), we give a general upper bound for the secrecy rate. This lemma is first motivated by, and stated for, the Gaussian wiretap channel with M helpers (see Fig. 2), which 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, $\mathrm{E}[X_i^2] \leq P$, for $i = 1, \ldots, M+1$. Transmitter 1 intends to send a message W to the legitimate receiver (receiver 1). The rate of the message is $R \triangleq (1/n)\log|\mathcal{W}|$, where n is the number of channel uses. 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, and the message is kept information-theoretically secure against the eavesdropper

$$\frac{1}{n} H(W|\mathbf{Y}_2) \geq \frac{1}{n} H(W) - \epsilon \tag{3}$$

[1]Very recently, the multiple access channel [62] and the interference channel with an external eavesdropper [63] have been considered for the case of no eavesdropper CSI at the transmitters.

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. This is equivalent to

$$\frac{1}{n} I(W; \mathbf{Y}_2) \leq \epsilon \tag{4}$$

i.e., the (normalized) information leakage to the eavesdropper asymptotically vanishes, resulting in perfect (weak) secrecy [3]. The supremum of all achievable secrecy rates is the secrecy capacity C_s, and the s.d.o.f., D_s, is defined as

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

The s.d.o.f. determines the scaling of the secrecy capacity with the capacity of a single-user channel which is $(1/2)\log P$ at high SNR. That is, s.d.o.f. is the prelog factor of the secrecy capacity at high SNR.

The goal of Lemma 1 is to quantify the *secrecy penalty* due to the presence of an eavesdropper. We work with n-letter signals (hence bold vectors) and introduce small independent Gaussian fudge variables $\tilde{N}_i$ and state inequalities in terms of slightly perturbed channel inputs $\tilde{X}_i$; this is for regularity purposes only, so that we can use differential entropies even for discrete signals throughout the paper.

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 (6). This upper bound can 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 (7).

Lemma 1 [46], [48]: [Secrecy penalty lemma] The secrecy rate of the legitimate pair is upper bounded as

$$nR \leq \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc \tag{6}$$

$$\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{7}$$

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.

In the following lemma (Lemma 2), we give a general upper bound for the differential entropy of the signal of a helper based on the decodability of the message of the legitimate transmitter at the legitimate receiver. This lemma is also motivated in the helper setting, but as with Lemma 1 above, it is valid for more general settings. The goal of this lemma is to quantify the *role of a helper*, in terms of its affect on the system. In this lemma, W is the message of the legitimate transmitter, and its entropy $H(W)$ is the message rate. Here, X_j is the jth helper's channel input, and Y_1 is the legitimate receiver's channel output. Again, we use slightly perturbed channel inputs for regularity.

This lemma is motivated as follows: 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 Y_1, there must exist a constraint on the cooperative jamming signal of the helper, X_j. This lemma develops a constraint on the differential entropy of (the noisy version of) the cooperative jamming signal of any given helper, helper j in (8), in terms of the differential entropy of the legitimate user's channel output and the message rate $H(W)$. The inequality in (8) states that, for a given message rate $H(W)$, the entropy of the signal that the helper puts into the channel should not be too much. Alternatively, $H(W)$ can be moved to the left hand side of (8), and this inequality can be interpreted as an upper on the message rate given the helper signal's entropy. In particular, the higher the differential entropy of the cooperative jamming signal the lower this upper bound on the message rate will be. This motivates us not to use i.i.d. Gaussian cooperative jamming signals which have the highest differential entropy.

Lemma 2 [46], [48]: [Role of a helper lemma] For reliable decoding at the legitimate receiver, the differential entropy of the input signal of helper j, $\mathbf{X}_j$, must satisfy

$$h(\mathbf{X}_j + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_1) - H(W) + nc \tag{8}$$

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

B. Achievability Tools: Real Interference Alignment

In this subsection, we review pulse amplitude modulation (PAM) and real interference alignment [60], [61], similar to the review in [45, Section III]. The purpose of this subsection is to illustrate that by using real interference alignment, the transmission rate of a PAM scheme can be made to approach the Shannon achievable rate at high SNR. This provides a universal and convenient way to design capacity-achieving signalling schemes at high SNR by using PAM for different channel models as will be done in later sections.

For a point-to-point scalar Gaussian channel

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

with additive Gaussian noise Z of zero-mean and variance σ^2, and an input power constraint $\mathrm{E}[X^2] \leq P$, assume that the input symbols are drawn from a PAM constellation

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

where Q is a positive integer and a is a real number to normalize the transmit power. Note that, a is also the minimum distance $d_{\min}(C)$ of this constellation, which has the probability of error

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

where $\hat{X}$ is an estimate for X obtained by choosing the closest point in the constellation $C(a, Q)$ based on observation Y.

This PAM scheme for the point-to-point scalar channel can be generalized to multiple data streams. Let the transmit signal be

$$x = \mathbf{a}^T\mathbf{b} = \sum_{i=1}^{L} a_i b_i \tag{12}$$

where $a_1, \ldots, a_L$ are rationally independent real numbers[2] and each b_i is drawn independently from the constellation $C(a, Q)$ in (10). The real value x is a combination of L data streams, and the constellation observed at the receiver consists of $(2Q+1)^L$ signal points.

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

By using the Khintchine–Groshev theorem of Diophantine approximation in number theory, [60], [61] bounded the minimum distance d_{min} of points in the receiver's constellation: For any $\delta > 0$, there exists a constant k_δ, such that

$$d_{\min} \geq \frac{k_\delta a}{Q^{L-1+\delta}} \tag{13}$$

for almost all rationally independent $\{a_i\}_{i=1}^{L}$, except for a set of Lebesgue measure zero. Since the minimum distance of the receiver constellation is lower bounded, with proper choice of a and Q, the probability of error can be made arbitrarily small, with rate R approaching $(1/2)\log P$. This result is stated in the following lemma, as in [45, Proposition 3].

Lemma 3 [60], [61]: [Real interference alignment] For any small enough $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose

$$Q = P^{\frac{1-\delta}{2(L+\delta)}} \quad \text{and} \quad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{14}$$

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

$$\Pr(e) \leq \exp(-\eta_\gamma P^\delta) \tag{15}$$

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

III. WIRETAP CHANNELS WITH M HELPERS

In this section, we consider the Gaussian wiretap channel with M helpers shown in Fig. 2 and defined in (1) and (2).

In the sequel, we will demonstrate the use of converse and achievability lemmas presented in Section II in some depth in the context of a helper network; we will then make much briefer presentations for the multiple access and interference networks in the following sections.

Here, we show that for the wiretap channel with M helpers, the exact s.d.o.f. is $M/(M+1)$, as stated in the following theorem. This shows that even though the helpers are independent, the s.d.o.f. increases monotonically with the number of helpers M, and goes to 1, which is the d.o.f. with no secrecy constraints.

Theorem 1 [46], [48]: The s.d.o.f. of the Gaussian wiretap channel with M helpers is $M/(M+1)$ for almost all channel gains.

A. Converse

We start with (7) of Lemma 1 with the selection of $j=1$

$$nR \le \sum_{i=1,i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{16}$$

$$= \sum_{i=2}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{17}$$

$$\le M[h(\mathbf{Y}_1) - H(W)] + nc_1 \tag{18}$$

where (18) is due to Lemma 2 for each cooperative jamming signal $\tilde{\mathbf{X}}_i$, $i=2,\cdots,M+1$. By noting $H(W)=nR$, (18) implies that

$$(M+1)nR \le Mh(\mathbf{Y}_1) + nc_1 \tag{19}$$

$$\le M\left(\frac{n}{2}\log P\right) + nc_2 \tag{20}$$

which further implies that

$$D_s \le \frac{M}{M+1} \tag{21}$$

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 $C(a,Q)$ in (10), where a and Q will be specified later. We choose the input signal of the legitimate transmitter as

$$X_1 = \sum_{k=2}^{M+1} \frac{g_k}{g_1 h_k} V_k \tag{22}$$

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

$$X_j = \frac{1}{h_j} U_j. \tag{23}$$

Then, the observations of the receivers are

$$Y_1 = \sum_{k=2}^{M+1} \frac{h_1 g_k}{g_1 h_k} V_k + \left[\sum_{j=2}^{M+1} U_j\right] + N_1 \tag{24}$$

$$Y_2 = \sum_{k=2}^{M+1} \frac{g_k}{h_k}[V_k + U_k] + N_2. \tag{25}$$

The intuition here is as follows: We use M independent subsignals V_k, $k=2,\cdots,M+1$, to represent the signals carrying 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 subsignal 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, $\{1, (h_1g_2/g_1h_2), (h_1g_3/g_1h_3), \cdots, (h_1g_{M+1}/g_1h_{M+1})\}$ are rationally independent, signals $\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=2}^{M+1} U_j\}$ can be distinguished by the legitimate receiver. Square parentheses in (24) and (25) indicate alignments at the two receivers. As an example, the case of $M=2$ is shown in Fig. 5.

The exact performance analysis supporting the above intuition is based on real interference alignment summarized in Lemma 3, and the achievable secrecy rate in [3]. In particular, 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 [3]

$$C_s \ge I(X_1;Y_1) - I(X_1;Y_2). \tag{26}$$

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 subsignal 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 Lemma 3, for any small enough $\delta>0$ and for almost all rationally independent $\{1, (h_1g_2/g_1h_2), (h_1g_3/g_1h_3), \cdots, (h_1g_{M+1}/g_1h_{M+1})\}$, except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q=P^{(1-\delta)/2(M+1+\delta)}$ and $a=\gamma P^{1/2}/Q$ then the average power constraint is satisfied and the probability of error is bounded as

$$\Pr[X_1 \neq \hat{X}_1] \le \exp(-\eta_\gamma P^\delta) \tag{27}$$

where η_γ is a positive constant which is independent of P and where $\hat{X}_1$ is the estimate of X_1 by choosing the closest point in the constellation based on observation Y_1. This

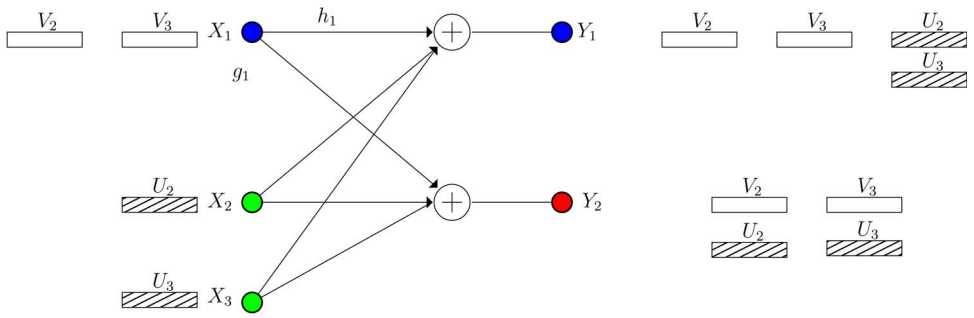


Fig. 5. *Illustration of interference alignment for the Gaussian wiretap channel with M helpers. Here, M = 2.*

shows that the legitimate receiver can decode the messages reliably.

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

$$H(X_1|Y_1) \le H(X_1|\hat{X}_1) \tag{28}$$

$$\le 1 + \exp(-\eta_\gamma P^\delta) \log(2Q+1)^M \tag{29}$$

which means that

$$I(X_1;Y_1) = H(X_1) - H(X_1|Y_1) \tag{30}$$

$$\ge \left[1 - \exp(\eta_\gamma P^\delta)\right] \log(2Q+1)^M - 1 \tag{31}$$

On the other hand

$$I(X_1;Y_2) \le I\left(X_1; \sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) \tag{32}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\middle| X_1\right) \tag{33}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k+U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}U_k\right) \tag{34}$$

$$\le \log(4Q+1)^M - \log(2Q+1)^M \tag{35}$$

$$\le M \log \frac{4Q+1}{2Q+1} \tag{36}$$

$$\le M \tag{37}$$

where (35) is due to the fact that entropy of the sum $\sum_{k=2}^{M+1}(g_k/h_k)(V_k+U_k)$ is maximized by the uniform distribution which takes values over a set of cardinality $(4Q+1)^M$.

Combining (31) and (37), from (26), we have

$$C_s \ge I(X_1;Y_1) - I(X_1;Y_2) \tag{38}$$

$$\ge \left[1 - \exp(-\eta_\gamma P^\delta)\right] \log(2Q+1)^M - (M+1) \tag{39}$$

$$\ge \left[1 - \exp(-\eta_\gamma P^\delta)\right] \log(2P^{\frac{1-\delta}{2(M+1+\delta)}}+1)^M - (M+1) \tag{40}$$

$$= \frac{M(1-\delta)}{(M+1+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{41}$$

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

IV. MULTIPLE ACCESS WIRETAP CHANNEL

In this section, we consider the K-user multiple access wiretap channel shown in Fig. 3, which has multiple transmitters each with its own message to transmit

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{42}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2. \tag{43}$$

We show that the exact sum s.d.o.f. of this channel is $K(K-1)/(K(K-1)+1)$, as stated in the following theorem. Note that this is strictly larger than the s.d.o.f. of the corresponding helper network, which is $(K-1)/K$.

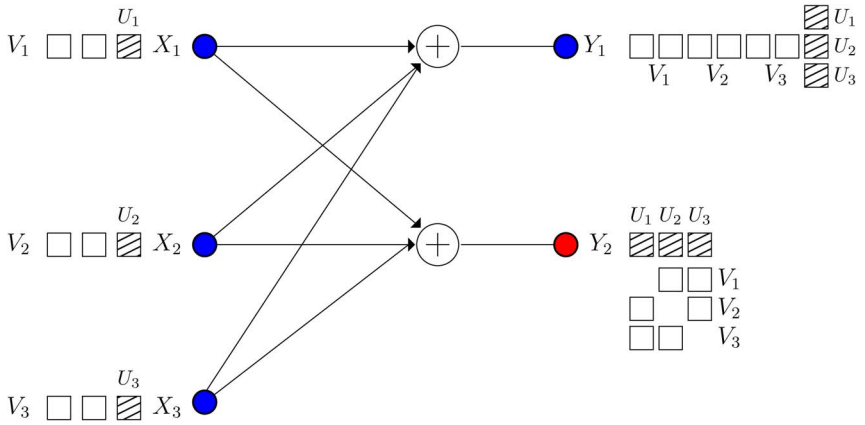


Fig. 6. *Illustration of interference alignment for the K-user multiple access wiretap channel. Here, $K = 3$.*

Theorem 2 [47], [48]: The sum s.d.o.f. of the K-user Gaussian multiple access wiretap channel is $K(K-1)/(K(K-1)+1)$ for almost all channel gains.

The converse is derived by starting with an upper bound which is similar to the *secrecy penalty* lemma in Lemma 1, and considering all transmitters as a single virtual transmitter

$$n\sum_{i=1}^{K} R_i \leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc_3 \tag{44}$$

$$\leq \sum_{i=2}^{K} h(\tilde{\mathbf{X}}_i) + nc_4. \tag{45}$$

In addition, similar to the *role of a helper* lemma in Lemma 2, we bound the differential entropy of each user's channel input with the sum of the decodable rates of all other users

$$\sum_{i\neq j} H(W_i) = H(W_{\neq j}) \leq h(\mathbf{Y}_1) - h(\tilde{\mathbf{X}}_j) + nc_5. \tag{46}$$

The converse is completed by proceeding similarly to the case of the helper network, starting from the above generalizations of Lemmas 1 and 2.

The achievable scheme is as follows: Each transmitter i divides its message into $K-1$ mutually independent subsignals. In addition, each transmitter i sends a cooperative jamming signal U_i. This is an instance of *channel prefixing* [3], where the channel input is further randomized. At the eavesdropper Y_2, each subsignal indexed by (i,j), where $j \in \{1,\cdots,K\}\setminus\{i\}$, 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 Fig. 6 for the case of $K = 3$.

Specifically, we use in total K^2 mutually independent random variables which are

$$V_{i,j}, \quad i,j \in \{1,2,\ldots,K\},\ j \neq i \tag{47}$$

$$U_k, \quad k \in \{1,2,\ldots,K\} \tag{48}$$

where $V_{i,j}$, $j \neq i$ are the $K-1$ subsignals that carry the message of user i, and U_i is the cooperative jamming signal sent by user i. All of these random variables are uniformly and independently drawn from the same constellation $C(a,Q)$ in (10). For each $i \in \{1,2,\ldots,K\}$, we choose the input signal of transmitter i as

$$X_i = \sum_{j=1,j\neq i}^{K} \frac{g_j}{g_i h_j} V_{i,j} + \frac{1}{h_i} U_i. \tag{49}$$

With these input signal selections, received signals are

$$Y_1 = \sum_{i=1}^{K}\sum_{j=1,j\neq i}^{K} \frac{g_j h_i}{g_i h_j} V_{i,j} + \left[\sum_{k=1}^{K} U_k\right] + N_1 \tag{50}$$

$$Y_2 = \left(\sum_{i=1}^{K}\sum_{j=1,j\neq i}^{K} \frac{g_j}{h_j} V_{i,j}\right) + \sum_{j=1}^{K} \frac{g_j}{h_j} U_j + N_2 \tag{51}$$

$$= \sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1,i\neq j}^{K} V_{i,j}\right] + N_2. \tag{52}$$

Each of the signals in the square parentheses in (50) and (52) are *aligned* in the same irrational *dimension*. This alignment in (50) ensures that the cooperative jamming signals occupy the smallest possible space at the legitimate receiver, and the alignment in (52) ensures that each U_j protects all the $V_{i,j}$s in the same square parentheses.

V. INTERFERENCE CHANNEL WITH SECRECY

In this section, we consider the K-user Gaussian interference channel with secrecy constraints shown in Fig. 4. The channel model is

$$Y_i = \sum_{j=1}^{K} h_{ji} X_j + N_i, \quad i = 1, \ldots, K \tag{53}$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \quad \text{(if there is any)} \tag{54}$$

which has not only multiple transmitters but also multiple receivers in the network. We consider three different secrecy requirements: interference channel with an external eavesdropper (IC-EE), where all of the messages are kept secure against the external eavesdropper; interference channel with confidential messages (IC-CM), where all messages are kept secure against unintended receivers; and their combination (IC-CM-EE), where all messages are kept secure against all unintended receivers and the eavesdropper. The sum s.d.o.f. is the same for all three networks and is stated in the following theorem.

Theorem 3 [49], [50]: The sum s.d.o.f. of the K-user IC-EE, IC-CM, and IC-CM-EE is $K(K-1)/(2K-1)$ for almost all channel gains.

We provide an outline of the converse and achievable scheme for IC-EE only here. The converse starts with Lemma 1, the *secrecy penalty* lemma: For any $j = 1, \ldots, K$

$$n \sum_{i=1}^{K} R_i \leq h\left(\tilde{\mathbf{X}}_1^K\right) - h(\mathbf{Z}) + nc_3 \tag{55}$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Z}) + nc_3 \tag{56}$$

$$\leq \sum_{i=1, i\neq j}^{K} h(\tilde{\mathbf{X}}_i) + nc_6. \tag{57}$$

Then, we apply the *role of a helper* lemma, Lemma 2, to each $\tilde{\mathbf{X}}_i$ with $k = i+1$ (for $i = K$, $k = 1$), in (57) as

$$n \sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + \cdots + h(\tilde{\mathbf{X}}_{j-1}) + h(\tilde{\mathbf{X}}_{j+1}) + \cdots + h(\tilde{\mathbf{X}}_K) + nc_7 \tag{58}$$

$$\leq [h(\mathbf{Y}_2) - nR_2] + [h(\mathbf{Y}_3) - nR_3] + \cdots + \left[h(\mathbf{Y}_j) - nR_j\right] + \left[h(\mathbf{Y}_{j+2}) - nR_{j+2}\right] + \cdots + [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + nc_8. \tag{59}$$

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

$$2n \sum_{i=1}^{K} R_i \leq (K-1)\left(\frac{n}{2}\log P\right) + nR_{(j+1) \bmod K} + nc_9 \tag{60}$$

for $j = 1, \ldots, K$. Therefore, we have a total of K bounds in (60) for $j = 1, \ldots, K$. Summing these K bounds, we obtain

$$(2K-1)n \sum_{i=1}^{K} R_i \leq K(K-1)\left(\frac{n}{2}\log P\right) + nc_{10} \tag{61}$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{62}$$

completing the converse for IC-EE.

The achievability is based on Lemma 3 for the K-user IC-CM-EE, which will imply achievability for K-user IC-EE. We employ a total of K^2 random variables

$$V_{ij}, \quad i, j = 1, \ldots, K, \quad j \neq i \tag{63}$$

$$U_k, \quad k = 1, \ldots, K \tag{64}$$

which are illustrated in Fig. 7 for the case of $K = 3$. For transmitter i, $K-1$ random variables $\{V_{ij}\}_{j\neq i}$, each representing a submessage, collectively carry message W_i. Different than before, rather than protecting one message at one receiver, each U_k simultaneously protects a portion of all submessages at all required receivers. More specifically, U_k protects $\{V_{ik}\}_{i\neq k, i\neq j}$ at receivers j, and at the eavesdropper (if there is any). For example, in Fig. 7, U_1 protects V_{21} and V_{31} where necessary. In particular, U_1 protects V_{21} at receivers 1, 3 and the eavesdropper; and it

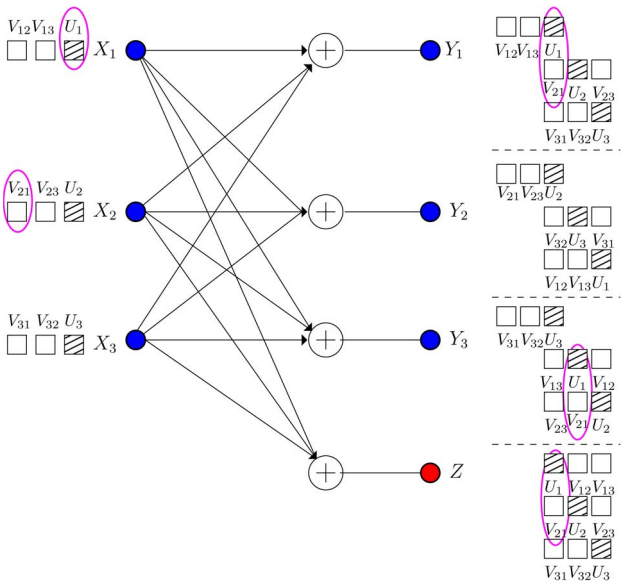


Fig. 7. *Illustration of alignment for 3-user IC-CM-EE. U_1 and V_{21} are marked to emphasize their simultaneous alignment at Y_1, Y_3 and Z.*

protects V_{31} at receivers 1, 2 and the eavesdropper. As a technical challenge, this requires U_1 to be aligned with the same signal, say V_{21}, at multiple receivers simultaneously, i.e., at receivers 1, 3 and the eavesdropper. These particular alignments are circled by ellipsoids in Fig. 7. We do these simultaneous alignments using asymptotic real alignment technique proposed in [61] and used in [38], [45].

VI. S.D.O.F. REGIONS OF WIRELESS NETWORKS

In this section, we revisit the K-user multiple access wiretap channel in Section IV and K-user interference channel in Section V, and study the s.d.o.f. *regions* of both networks. The results have been characterized in the following theorems.

Theorem 4 [51], [53]: The s.d.o.f. region D of the K-user multiple access wiretap channel is the set of all $\mathbf{d}$ satisfying

$$Kd_i + (K-1)\sum_{j=1,j\neq i}^{K} d_j \leq K-1, \quad i=1,\ldots,K \tag{65}$$

$$d_i \geq 0, \quad i=1,\ldots,K \tag{66}$$

for almost all channel gains.

Theorem 5 [52], [53]: The s.d.o.f. region D of K-user IC-EE, IC-CM, and IC-CM-EE is the set of all $\mathbf{d}$ satisfying

$$Kd_i + \sum_{j=1,j\neq i}^{K} d_j \leq K-1, \quad i=1,\ldots,K \tag{67}$$

$$\sum_{i\in V} d_i \leq 1, \quad \forall\, V\subseteq\{1,\ldots,K\},\ |V|=2 \tag{68}$$

$$d_i \geq 0, \quad i=1,\ldots,K \tag{69}$$

for almost all channel gains.

The complete proofs can be found in [51]–[53]. The major challenge in the proofs of both theorems is to show the tightness of the converse regions. We first note that the converse regions have *polytope* structures. This is because: A set $P\subseteq R^n$ is a *polyhedron* if there is a system of finitely many inequalities $\mathbf{Hx}\leq\mathbf{h}$ such that

$$P=\{\mathbf{x}\in R^n|\mathbf{Hx}\leq\mathbf{h}\} \tag{70}$$

Further, if P is a bounded polyhedron, then it is a polytope, which is the case for the converse regions we derive. Due to the Minkowski theorem below, the converse regions are equal to the convex hull of their corresponding extreme points.

Theorem 6 (Minkowski, 1910 [64, Theorem 2.4.5]): Let $P\subseteq R^n$ be a compact convex set. Then

$$P=Co(Ex(P)). \tag{71}$$

Minkowski theorem plays an important role in this problem, since it tells that, instead of studying the polytope P itself, for this problem, i.e., achievability proofs, we can simply concentrate on all extreme points $\mathrm{Ex}(P)$. The following theorem helps us find all extreme points of a polytope P efficiently: We select any n linearly independent active/tight boundaries and check whether they give a point in the polytope P.

Theorem 7 [65, Theorem 7.2(b)]: $\mathbf{x}\in R^n$ is an extreme point of polyhedron $P(\mathbf{H},\mathbf{h})$ if and only if $\mathbf{Hx}\leq\mathbf{h}$ and $\mathbf{H}'\mathbf{x}=\mathbf{h}'$ for some $n\times(n+1)$ submatrix $(\mathbf{H}',\mathbf{h}')$ of $(\mathbf{H},\mathbf{h})$ with $\mathrm{rank}(\mathbf{H}')=n$.

As shown by the proof in [53], the s.d.o.f. region of the multiple access wiretap channel is constrained by secrecy constraints only. However, different portions of the s.d.o.f. region of the interference channel are governed by different upper bounds. To see this, we can study the structure of the extreme points of D, since D is the convex

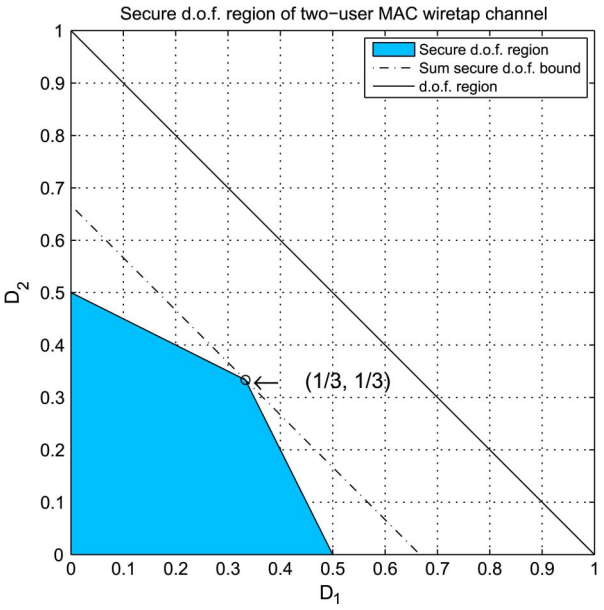


Fig. 8. *The s.d.o.f. region of the $K = 2$-user multiple access wiretap channel.*

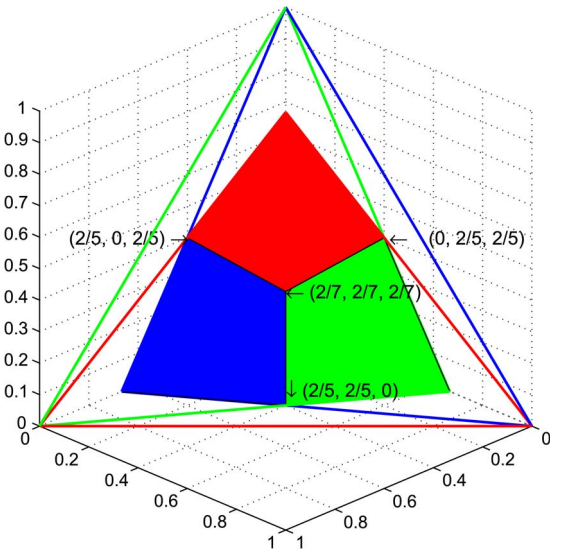


Fig. 9. *The s.d.o.f. region of the $K = 3$-user multiple access wiretap channel.*

hull of them. The sum s.d.o.f. tuple, which is symmetric and has no zero elements, is governed by the upper bounds in (67) due to secrecy constraints. However, as shown in [53], all other extreme points have zeros as some elements, and therefore are governed by the upper bounds in (68) due to interference constraints in [66] and [67]. An explanation can be provided as follows: When some transmitters do not have messages to transmit, we may employ them as "helpers." Even though secrecy constraint is considered in our problem, with the help of the "helpers," the effect due to the existence of the eavesdropper in the network can be *eliminated*. Hence, this portion of the s.d.o.f. region is dominated by the interference constraints.

Here, as concrete examples, we provide the s.d.o.f. regions for the multiple access wiretap channel and the interference channel with secrecy constraints when $K = 2$, 3, 4, to show intricate differences. The detailed proofs and the structures of the extreme points for all K can be found in [53].

For $K = 2$, the s.d.o.f. region of the multiple access wiretap channel in Theorem 4 becomes

$$D = \{\mathbf{d} : 2d_1 + d_2 \leq 1,\ d_1 + 2d_2 \leq 1, d_1, d_2 \geq 0\} \quad (72)$$

and is shown in Fig. 8. The extreme points of this region are: $(0,0), (1/2,0), (0,1/2)$, and $(1/3,1/3)$. In order to provide the achievability of the region, it suffices to provide the achievability of these extreme points. In fact, the achievabilities of $(1/2,0), (0,1/2)$ were proved in [46] and [48] in the helper setting and the achievability of $(1/3,1/3)$ was proved in [47] and [48]. Note that $(1/3,1/3)$ is the only sum s.d.o.f. optimum point.

For $K = 3$, the s.d.o.f. region of the multiple access wiretap channel in Theorem 4 becomes

$$D = \{\mathbf{d} : 3d_1 + 2d_2 + 2d_3 \leq 2,\ 2d_1 + 3d_2 + 2d_3 \leq 2, \\ 2d_1 + 2d_2 + 3d_3 \leq 2,\ d_1, d_2, d_3 \geq 0\} \quad (73)$$

and is shown in Fig. 9. The extreme points of this region are

$$\left(0,0,0\right) \\ \left(\frac{2}{3},0,0\right), \left(0,\frac{2}{3},0\right), \left(0,0,\frac{2}{3}\right) \\ \left(\frac{2}{5},\frac{2}{5},0\right), \left(\frac{2}{5},0,\frac{2}{5}\right), \left(0,\frac{2}{5},\frac{2}{5}\right) \\ \left(\frac{2}{7},\frac{2}{7},\frac{2}{7}\right) \quad (74)$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers [46], [48]), the maximum sum of pair of s.d.o.f. (see two-user Gaussian multiple access wiretap channel with one

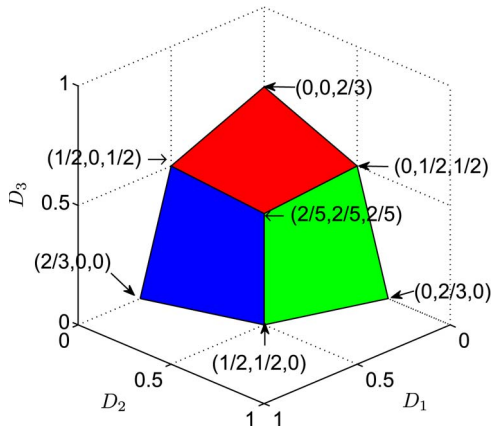


Fig. 10. *The s.d.o.f. region of the $K = 3$-user interference channel.*

helper, proved in [53]), and the maximum sum s.d.o.f. (see three-user Gaussian multiple access wiretap channel [47], [48]). Note that $(2/7, 2/7, 2/7)$ is the only sum s.d.o.f. optimum point.

For $K = 2$, the s.d.o.f. region of the interference channel with secrecy constraints in Theorem 5 becomes

$$D = \{\mathbf{d} : 2d_1+d_2 \leq 1,\ d_1+2d_2 \leq 1,\ d_1, d_2 \geq 0\} \quad (75)$$

which is the same as (72), and is shown in Fig. 8. Note that (68) is not necessary for the two-user case, since summing the bounds $2d_1 + d_2 \leq 1$ and $d_1 + 2d_2 \leq 1$ up gives a new bound

$$d_1 + d_2 \leq \frac{2}{3} \quad (76)$$

which is the result in Theorem 3 and makes the constraint in (68) strictly loose. In order to provide the achievability, it suffices to check that the extreme points $(0,0)$, $(1/2, 0)$, $(0, 1/2)$, and $(1/3, (1/3)$ are achievable. In fact, the achievabilities of $(1/2, 0)$, $(0, 1/2)$ are similar to [46] and [48] and shown in [53]. The achievability of $(1/3, 1/3)$ was proved in [49], [50]. Note that $(1/3, 1/3)$ is the only sum s.d.o.f. optimum point.

For $K = 3$, the s.d.o.f. region of the interference channel with secrecy constraints in Theorem 5 becomes

$$\begin{aligned} D = \{\mathbf{d} : 3d_1 + d_2 + d_3 \leq 2,\ d_1 + 3d_2 + d_3 \leq 2,\\ d_1 + d_2 + 3d_3 \leq 2,\ d_1, d_2, d_3 \geq 0\} \end{aligned} \quad (77)$$

which is shown in Fig. 10. Inequality in (68) is not necessary for the three-user case, either. This is because, due to the positiveness of each element in $\mathbf{d}$, from the first two inequalities in (77), we have

$$3d_1 + d_2 \leq 3d_1 + d_2 + d_3 \leq 2 \quad (78)$$

$$d_1 + 3d_2 \leq d_1 + 3d_2 + d_3 \leq 2. \quad (79)$$

Summing the left hand sides up of (78) and (79) gives us

$$d_1 + d_2 \leq 1 \quad (80)$$

which is (68) with $V = \{1, 2\}$, and we have (68) for free from (77). The extreme points of this region are

$$\begin{aligned} &\left(0, 0, 0\right)\\ &\left(\frac{2}{3}, 0, 0\right), \left(0, \frac{2}{3}, 0\right), \left(0, 0, \frac{2}{3}\right)\\ &\left(\frac{1}{2}, \frac{1}{2}, 0\right), \left(\frac{1}{2}, 0, \frac{1}{2}\right), \left(0, \frac{1}{2}, \frac{1}{2}\right)\\ &\left(\frac{2}{5}, \frac{2}{5}, \frac{2}{5}\right) \end{aligned} \quad (81)$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers [46], [48]), the maximum sum of pair of s.d.o.f. (proved in [53]), and the maximum sum s.d.o.f. (see three-user Gaussian IC-CM-EE in [49] and [50]). Note that, $(1/2, 1/2)$ is the maximum sum d.o.f. for a two-user IC *without* secrecy constraints, and $(2/5, 2/5, 2/5)$ is the only sum s.d.o.f. optimum point. Finally, note the difference of the extreme points of the 3-user interference channel in (81) from the corresponding 3-user multiple access wiretap channel in (74), even though the s.d.o.f. regions and the extreme points of the 2-user interference channel and 2-user multiple access wiretap channel in (75) and (72) were the same.

For $K = 4$, the s.d.o.f. region of the interference channel with secrecy constraints in Theorem 5 becomes

$$\begin{aligned} D = \{\mathbf{d} : &4d_1 + d_2 + d_3 + d_4 \leq 3,\ d_1 + 4d_2 + d_3 + d_4 \leq 3,\\ &d_1 + d_2 + 4d_3 + d_4 \leq 3,\ d_1 + d_2 + d_3 + 4d_4 \leq 3,\\ &d_1 + d_2 \leq 1,\ d_1 + d_3 \leq 1,\ d_1 + d_4 \leq 1,\\ &d_2 + d_3 \leq 1,\ d_2 + d_4 \leq 1,\ d_3 + d_4 \leq 1,\\ &d_1, d_2, d_3, d_4 \geq 0\}. \end{aligned} \quad (82)$$

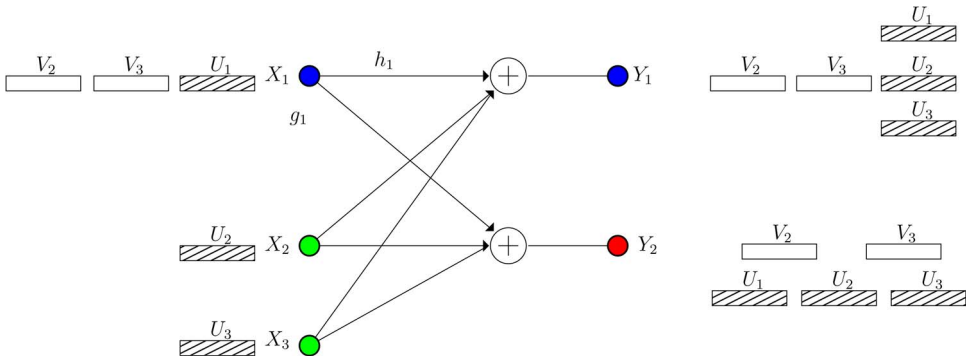


Fig. 11. *Illustration of the alignment scheme based on blind cooperative jamming for Gaussian wiretap channel with M helpers (eavesdropper's CSI is not available at the transmitters).*

The extreme points of this region are

$$\begin{aligned}
&\left(0,0,0,0\right)\\
&\left(\frac{3}{4},0,0,0\right),\left(0,\frac{3}{4},0,0\right),\left(0,0,\frac{3}{4},0\right),\left(0,0,0,\frac{3}{4}\right)\\
&\left(\frac{2}{3},\frac{1}{3},0,0\right)\quad\text{up to element reordering}\\
&\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},0\right),\left(\frac{1}{2},\frac{1}{2},0,\frac{1}{2}\right),\left(\frac{1}{2},0,\frac{1}{2},\frac{1}{2}\right),\left(0,\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)\\
&\left(\frac{3}{7},\frac{3}{7},\frac{3}{7},\frac{3}{7}\right).
\end{aligned}\tag{83}$$

Here, in contrast to the two-user and three-user cases, (68) is absolutely necessary. For example, the point $(3/5, 3/5, 0, 0)$ satisfies (67), but not (68). In fact, it cannot be achieved, and (68) is strictly needed to enforce that fact.

VII. HELPER NETWORK WITH NO EAVESDROPPER CSI: BLIND COOPERATIVE JAMMING

In this section, we consider the case where the legitimate transmitters do not have CSI of the channels to the eavesdropper. We present one more technical tool, *blind cooperative jamming*, which will be used to prove that, even in the case of no eavesdropper CSI at the transmitters, the s.d.o.f. of the Gaussian wiretap channel with M helpers is still $M/(M+1)$, as in the case of full eavesdropper CSI in Section III.

Theorem 8 [54]: The s.d.o.f. of the Gaussian wiretap channel with M helpers, but no eavesdropper CSI at the transmitters is $M/(M+1)$ for almost all channel gains.

The converse for this result follows from the converse for the case of full CSI, as the s.d.o.f. with full CSI is an upper bound for the s.d.o.f. without eavesdropper CSI.

When there is no eavesdropper CSI at the transmitters, the cooperative jamming signals cannot be aligned with the message carrying signals at the eavesdropper to protect them as in Fig. 5. In this case, the insight of *blind cooperative jamming* is that all of the $M+1$ transmitters send a large number of cooperative jamming signals, which get distributed to sufficiently many dimensions at the eavesdropper's observation space, exceeding its maximum decoding capability and protecting the message carrying signals; see Fig. 11. Then, the information leakage to the eavesdropper can be upper bounded by a function which vanishes as the transmit power P becomes large, using a method different than in Section III. In addition, the CSI of the channels to the legitimate receiver is used to align all of the $M+1$ cooperative jamming signals in the smallest possible dimension at the legitimate receiver.

Let $\{V_2, V_3, \ldots, V_{M+1}, U_1, U_2, U_3, \ldots, U_{M+1}\}$ be mutually independent discrete random variables, each of which uniformly drawn from the same PAM constellation $C(a, Q)$ in (10). We choose the input signal of the legitimate transmitter as

$$X_1 = \frac{1}{h_1}U_1 + \sum_{k=2}^{M+1}\alpha_k V_k \tag{84}$$

where $\{\alpha_k\}_{k=2}^{M+1}$ are rationally independent and independent of all channel gains. The input signal of the jth helper, $j = 2, \cdots, M+1$, is chosen as

$$X_j = \frac{1}{h_j}U_j. \tag{85}$$

Then, the observations of the receivers are

$$Y_1 = \sum_{k=2}^{M+1} h_1 \alpha_k V_k + \left[\sum_{j=1}^{M+1} U_j \right] + N_1 \quad (86)$$

$$Y_2 = \sum_{k=2}^{M+1} g_1 \alpha_k V_k + \sum_{j=1}^{M+1} \frac{g_j}{h_j} U_j + N_2 \quad (87)$$

where the signals in square parentheses in (86) are *aligned* at the legitimate receiver.

The intuition here is as follows: We use M independent subsignals V_k, $k = 2, \cdots, M+1$, to represent the original message W. The input signal X_1 is a linear combination of V_ks and a cooperative jamming signal U_1. 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 $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$ are rationally independent with probability one, the signals $\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=1}^{M+1} U_j\}$ can be distinguished by the legitimate receiver. Due to the fact that the eavesdropper's CSI is not available at the transmitters, the alignment-based achievable scheme in Section III does not work for this model. However, we observe that the coefficients $\{g_1/h_1, \cdots, g_{M+1}/h_{M+1}\}$ are rationally independent, and therefore, $\{U_1, U_2, \cdots, U_{M+1}\}$ *span* the *entire space* at the eavesdropper; see Fig. 11. Here, by *entire space*, we mean the maximum number of *dimensions* eavesdropper is capable to decode, which is $M+1$ in this case. Since the entire space at the eavesdropper is occupied by the cooperative jamming signals, the message signals $\{V_2, V_3, \ldots, V_{M+1}\}$ are protected.

We note that, while only the helpers sent cooperative jamming signals in the case of full eavesdropper CSI in Section III, here the legitimate transmitter also sends a cooperative jamming signal. These $M+1$ cooperative jamming signals are needed to protect M message carrying signals at the eavesdropper, i.e., the lack of CSI of the eavesdropper is compensated by increasing the number of cooperative jamming signals with respect to the number of message carrying signals.

VIII. CONCLUSION

In this review paper, we revisited the sum s.d.o.f. and s.d.o.f. regions of several one-hop wireless networks with secrecy constraints: Gaussian wiretap channel with helpers, Gaussian multiple access wiretap channel, and Gaussian interference channel with secrecy constraints. We first reviewed two key lemmas required for converse proofs. The *secrecy penalty* lemma showed that the net effect of an eavesdropper on the system is that it eliminates one of the independent channel inputs. The *role of a helper* lemma developed a direct relationship between the cooperative jamming signal of a helper and the message rate. We showed how to apply these two lemmas in the helper network in depth, and also in the IC-EE network briefly. We presented achievable schemes based on (asymptotic) real interference alignment, cooperative jamming, structured signalling, and also blind cooperative jamming in the case of no CSI at the transmitters in the helper network. We also reviewed the polytope structure of the s.d.o.f. converse regions, identified the extreme points, and then showed the achievability for each of the extreme points. ■

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[6] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

[7] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[9] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[11] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[12] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Mar. 2009, Art. no. 824235.

[13] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secure broadcasting: The secrecy rate region," presented at the 46th Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Sep. 2008.

[14] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[15] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865–1879, Apr. 2010.

[16] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," presented at the 43rd Annu. Conf. Inf. Sci. Syst., Baltimore, MD, USA, Mar. 2009.

[17] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[18] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5681–5694, Sep. 2011.

[19] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[20] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[21] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," presented at the 46th Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Sep. 2008.

[22] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

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

[24] Y. Oohama, "Relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Nov. 2006, pp. 87–89.

[25] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[26] M. Yuksel and E. Erkip, "The relay channel with a wiretapper," presented at the 41st Annu. Conf. Inf. Sci. Syst., Baltimore, MD, USA, Mar. 2007.

[27] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," presented at the IEEE Inf. Theory Workshop, Porto, Portugal, May 2008.

[28] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

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

[30] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[31] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forens. Sec.*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[32] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "Achievable secrecy rate regions for the two-way wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8099–8114, Dec. 2013.

[33] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, "Weak secrecy in the multiway untrusted relay channel with compute-and-forward," *IEEE Trans. Inf. Forens. Sec.*, vol. 10, no. 6, pp. 1262–1273, Jun. 2015.

[34] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 142374, Mar. 2009.

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

[36] X. He and A. Yener, "*K*-user interference channels: Achievable secrecy rate and degrees of freedom," presented at the IEEE Inf. Theory Workshop Netw. Inf. Theory, Volos, Greece, Jun. 2009.

[37] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[38] J. Xie and S. Ulukus, "Real interference alignment for the *K*-user Gaussian interference compound wiretap channel," presented at the 48th Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Sep. 2010.

[39] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[40] X. He, "Cooperation and Information Theoretic Security in Wireless Networks," Ph.D. dissertation, Pennsylvania State Univ., State College, PA, USA, 2010.

[41] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Mar. 2010, pp. 2588–2592.

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

[43] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," presented at the 46th Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Sep. 2008.

[44] J. Xie and S. Ulukus, "Sum secure degrees of freedom of two unicast layered wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1931–1943, Sep. 2013.

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

[46] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," presented at the 50th Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Oct. 2012.

[47] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," presented at the IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, Jul. 2013.

[48] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[49] J. Xie and S. Ulukus, "Unified secure DoF analysis of *K*-user Gaussian interference channels," presented at the IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, Jul. 2013.

[50] J. Xie and S. Ulukus, "Secure degrees of freedom of *K*-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[51] J. Xie and S. Ulukus, "Secure degrees of freedom region of the Gaussian multiple access wiretap channel," presented at the 47th Asilomar Conf. Signals, Syst., Comput., Pacific Grove, CA, USA, Nov. 2013.

[52] J. Xie and S. Ulukus, "Secure degrees of freedom region of the gaussian interference channel with secrecy constraints," presented at the IEEE Inf. Theory Workshop, Hobart, Tasmania, Australia, Nov. 2014.

[53] J. Xie and S. Ulukus, "Secure degrees of freedom region of wireless networks: The polytope structure," *IEEE Trans. Inf. Theory*, Apr. 2014, submitted.

[54] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," presented at the Conf. Inf. Sci. Syst., Baltimore, MD, Mar. 2013.

[55] J. Xie and S. Ulukus, "Inseparability of the multiple access wiretap channel," presented at the IEEE Int. Symp. Inf. Theory, Honolulu, HI, USA, Jun. 2014.

[56] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568–1571, Aug. 2013.

[57] M. Nafea and A. Yener, "How many antennas does a cooperative jammer need for achieving the degrees of freedom of multiple antenna Gaussian channels in the presence of an eavesdropper?" presented at the 51st Annu. Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Oct. 2013.

[58] M. Nafea and A. Yener, "Degrees of freedom of the single antenna gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper," presented at the IEEE GlobalSIP Symp. Cyber-Security Privacy, Austin, TX, USA, Dec. 2013.

[59] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," presented at the IEEE Int. Symp. Inf. Theory, Toronto, ON, Canada, Jul. 2008.

[60] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *IEEE Trans. Inf. Theory*, Aug. 2009, arXiv:0908.1208, submitted.

[61] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4799–4810, Aug. 2014.

[62] P. Mukherjee and S. Ulukus, "Secure degrees of freedom of the multiple access wiretap channel with no eavesdropper CSI," presented at the IEEE Int. Symp. Inf. Theory, Hong Kong, Jun. 2015.

[63] P. Mukherjee and S. Ulukus, "Secure degrees of freedom of the interference channel with no eavesdropper CSI," in *IEEE Inf. Theory Workshop*, Oct. 2015.

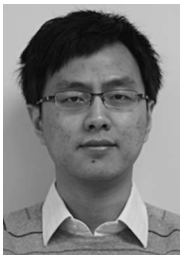
[64] B. Grunbaum, *Convex Polytopes*, 2nd ed. Berlin, Germany: Springer-Verlag, 2003.

[65] M. Padberg, *Linear Optimization and Extensions*, 2nd ed. Berlin, Germany: Springer-Verlag, 1999.

[66] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," presented at the IEEE Int. Symp. Inf. Theory, Adelaide, Australia, Sep. 2005.

[67] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the *K*-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

ABOUT THE AUTHORS



Jianwei Xie received the B.S. and M.S. degrees in electronic engineering from the Tsinghua University, Beijing, China, in 2006 and 2008, respectively. He received the Ph.D. degree from the Department of Electrical and Computer Engineering at the University of Maryland, College Park, MD, USA, in May 2014.

Currently, he is with Google Inc., Mountain View, CA, USA. He received the Distinguished Dissertation Fellowship from the ECE Department at the University of Maryland, College Park, in 2013. His research interests include information theory and wireless communications.

Sennur Ulukus (Member, IEEE) received the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, Ankara, Turkey, and the Ph.D. degree in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA.

She is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, College Park, MD, USA, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. Her research interests include wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information theoretic physical layer security, and energy harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, a 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE Transactions on Information Theory (2007–2010) and the IEEE Transactions on Communications (2003–2007). She served as a Guest Editor for the IEEE Journal on Selected Areas in Communications for the Special Issue on wireless communications powered by energy harvesting and wireless energy transfer (2015), the *Journal of Communications and Networks* for the Special Issue on energy harvesting in wireless networks (2012), the IEEE Transactions on Information Theory for the Special Issue on interference networks (2011), IEEE Journal on Selected Areas in Communications for the Special Issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC Cochair of the 2014 IEEE PIMRC, the Communication Theory Symposium at 2014 IEEE Globecom, the Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, the Physical-Layer Security Workshop at 2011 IEEE ICC, thr 2011 Communication Theory Workshop (IEEE CTW), thr Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and thr Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) from 2007 to 2009.