Real Interference Alignment for the K-User Gaussian Interference Compound Wiretap Channel

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

***Abstract*— We study the K-user Gaussian interference wiretap channel with N external eavesdroppers. All the transmitters, receivers and eavesdroppers have a single antenna each. We propose an achievable scheme to lower bound the secure degrees of freedom (d.o.f.) for each transmitter-receiver pair. Our approach is based on the (real) interference alignment technique. Our achievable scheme not only aligns the interference at each receiver to prevent the d.o.f. from vanishing, but also aligns the signals observed by the eavesdroppers to reduce the secrecy penalty. The achievable secure d.o.f. of each transmitter-receiver pair is shown to be $\frac{1}{2}-\frac{1}{2K}$ for almost all channel gains.**

I. Introduction

In his pioneering work [1], Wyner introduced the wiretap channel for secure communications, in which the transmitter wishes to send a message to the receiver secret from the eavesdropper. If the quality of the transmitter-receiver channel is *better* than that of the transmitter-eavesdropper channel, he showed that the messages can be transmitted securely at a positive rate. Later, this result was generalized by Csiszar *et. al.* [2] to broadcast channels with confidential messages and extended by Leung-Yan-Cheong *et. al.* [3] to Gaussian wiretap channels. In recent years, a considerable amount of research works studied secure communications over fading channels [4]–[6], over multi-antenna wiretap channels, with/without multi-user extensions [7]–[13].

To transmit secure information against more than one eavesdropper, [4], [14]–[16] studied the compound wiretap channel, in which one eavesdropper takes a number of channel states, or equivalently, there are multiple channels with multiple non-colluding eavesdroppers. In such a compound wiretap channel, the transmitter wishes to broadcast a common message to one or multiple legitimate receivers, but keep the information secret from all of the eavesdroppers. To satisfy the secrecy constraint, one achievable secrecy rate was derived by [14], where the *worst* receiver's channel and the *best* eavesdropper's channel dominate the secrecy rate. However, this rate is not always positive in general. When multiple antennas are employed, using the real interference alignment technique introduced in [17], [18], reference [16] developed a lower bound on the secure degrees of freedom (d.o.f.) for the multiple-input-single-output (MISO) compound wiretap channel, and showed that it is strictly positive. In this model, the transmitter which is equipped with M antennas broadcasts a common message to J_1 legitimate receivers, and there are J_2 eavesdroppers listening to this channel. All the receivers and the eavesdroppers have a single antenna each. The lower bound on the secure d.o.f. is $1-\frac{1}{M}$, which does not vanish as the number of eavesdroppers increases.

By examining the proposed achievable scheme in [16] carefully, we note that the constructed wiretap code does not rely on cooperation between the multiple antennas of the transmitter. Therefore, one could straightforwardly consider a new channel model consisting of K transmitters (with a single antenna each), K receivers, and N eavesdroppers, i.e., multiple transmitters and receivers wanting to communicate securely against an arbitrary number of eavesdroppers. Assuming that each receiver wishes to know the message only from one specific transmitter, using the same scheme, one could achieve secure d.o.f. of $\frac{1}{K}(1-\frac{1}{K})$ per transmitter-receiver pair, which vanishes as K increases. This turns out to be an interference network problem with secrecy constraints. Our goal in this paper is to extend the achievable scheme in [16] in a way to improve the achievable secure d.o.f. in an interference compound wiretap channel, by simultaneously aligning interference at the receivers and the eavesdroppers in a favorable manner. We show that a secure d.o.f. which does not vanish with the number of legitimate pairs or the number of eavesdroppers can be achieved.

In an interference network, there are K transmitter-receiver pairs sharing the channel, and each transmitter has data intended only for one specific receiver. Without secrecy constraints, many works [17]–[22] studied the capacity or achievable schemes in terms of d.o.f. for this channel model. Following the work of Cadambe and Jafar [19], in which the interference alignment scheme was proposed to achieve $\frac{1}{2}$ d.o.f. per transmitter-receiver pair for the K-user interference fading channel, several works developed similar ideas to achieve $\frac{1}{2}$ d.o.f. under different fading channel settings, such as the ergodic fading channel [20]. In [22], authors showed that $\frac{1}{2}$ d.o.f. per transmitter-receiver pair is achievable even for time-invariant interference channels if the channel coefficients are irrational numbers. Based on the same mathematical tool in number theory, references [17], [18] developed the real interference alignment technique to achieve $\frac{1}{2}$ d.o.f. per transmitter-receiver pair for time-

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

invariant interference channels almost surely.

In this work, we consider a K-user interference compound wiretap channel, and develop an interference alignment scheme which achieves a d.o.f. which does not vanish as the number of legitimate pairs and/or the number of eavesdroppers increase. Several works [23]–[27] studied the K-user interference channel with confidential messages. This is the model where there are no external eavesdroppers, but all messages are kept secret from unintended receivers under different secrecy constraints [23]. Some closely related works [24]–[28] studied the K-user interference channel with only one external eavesdropper. In [24], [25], it was shown that positive secure d.o.f. is achievable for the class of fading interference channels with one external eavesdropper. In [26], [27], it was shown that structured codes can achieve positive secure d.o.f. for the two-user time-invariant interference channel with an external eavesdropper. In [28], authors established the achievable secrecy rate region for the K-user time-invariant Gaussian multiple access channel with an external eavesdropper. In [16], the positive achievable secure d.o.f. was derived for the class of time-invariant MISO wiretap channels with multiple external eavesdroppers, in which a single transmitter with multiple antennas broadcasts secure common messages to multiple receivers. Besides the different channel models, the techniques in these works are different. References [23]–[25] utilized multiple symbol extensions for the fading channel to align the interference, whereas [16]–[18], [28] exploited the real interference alignment technique to align the interference in time-invariant channels.

In this work, we employ the real interference alignment technique to achieve positive secure d.o.f. per transmitter-receiver pair for almost all the K-user time-invariant scalar Gaussian interference channels with N external eavesdroppers. We show that the achieved secure d.o.f. does not vanish as K, N increase. The key insight of our scheme is to exploit the interference alignment idea not only to align the interference at legitimate receivers to prevent the d.o.f. from vanishing as K increases, but also to align the signals observed by the eavesdroppers to occupy smaller *dimensions* to reduce the secrecy penalty.

II. Channel Model

There are K legitimate transmitter-receiver pairs and N eavesdroppers. The input-output relations for this K-user Gaussian interference compound wiretap channel are:

$$y_j = \sum_{i=1}^{K} h_{ji} x_i + v_j \quad \text{and} \quad z_k = \sum_{i=1}^{K} g_{ki} x_i + w_k \tag{1}$$

where x_i is the transmitted symbol from transmitter i for $i = 1, 2, \ldots, K$, y_j is the received symbol at receiver j for $j = 1, 2, \ldots, K$, and z_k is the received signal at eavesdropper k for $k = 1, 2, \ldots, N$, respectively. h_{ji} and g_{ki} are the channel coefficients from transmitter i to receiver j and eavesdropper k, respectively. Each transmitter has a power constraint P. In addition, $\{v_j\}$ and $\{w_k\}$ are mutually independent additive white Gaussian noises with unit variance.

In this paper, we are interested to explore the achievable secure d.o.f. for each transmitter-receiver pair. Assume that, for every transmitter-receiver pair i, the transmitter i has a message m_i and encodes it into an n-length channel input sequence x_i^n, uniformly distributed over a set of size 2^{nR_s}. Receiver i decodes the message and has an estimate $\hat{m}_i$. R_s is an achievable secrecy rate for each transmitter-receiver pair provided that the probability of error $P_{e,i} = \Pr(m_i \neq \hat{m}_i) \to 0$ for each transmitter-receiver pair i, and equivocation rate $\frac{1}{n} H(m_1, m_2, \ldots, m_K | z_k^n) \geq K R_s - \delta$ for all eavesdroppers $k \in \{1, 2, \ldots, N\}$ where $\delta \to 0$ as $n \to \infty$. We denote the achievable secure d.o.f. for each transmitter-receiver pair by d:

$$d = \limsup_{P \to \infty} \frac{R_s}{\frac{1}{2} \log P} \tag{2}$$

We claim that there is an achievable secrecy rate $R_s = \frac{K-1}{4K} \log P + o(\log P)$ and the corresponding achievable secure d.o.f. is

$$d = \frac{1}{2} - \frac{1}{2K} \tag{3}$$

almost surely, where o is the little-o function such that $\lim_{t \to \infty} o(t)/t = 0$.

III. Preliminaries

A. Pulse Amplitude Modulation

For a point-to-point scalar channel,

$$y = x + z \tag{4}$$

where the input has a power constraint $\mathrm{E}\left[x^2\right] \leq P$ and additive Gaussian noise $z \sim \mathcal{N}(0, \sigma^2)$. Assume that the input symbols are drawn from a PAM constellation,

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{5}$$

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

$$P_e \leq \exp\left(-\frac{d_{min}^2}{8\sigma^2}\right) = \exp\left(-\frac{a^2}{8\sigma^2}\right) \tag{6}$$

The transmission rate of this PAM scheme is

$$R = \log(2Q + 1) \tag{7}$$

For any small enough $\epsilon > 0$, if we choose $Q = P^{\frac{1-\epsilon}{2}}$ and $a = \gamma P^{\frac{\epsilon}{2}}$, where γ is a constant independent of P, then

$$P_e \leq \exp\left(-\frac{\gamma^2 P^{\epsilon}}{8\sigma^2}\right) \quad \text{and} \quad R \geq \frac{1-\epsilon}{2} \log P \tag{8}$$

and we can have $P_e \to 0$ and $R \to \frac{1}{2} \log P$ as $P \to \infty$. That is, we can have reliable communication at rates approaching $\frac{1}{2} \log P$, and therefore have 1 d.o.f.

B. Real Interference Alignment

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

signal be

$$x = \mathbf{a}^T \mathbf{b} = \sum_{i=1}^{L} a_i b_i \tag{9}$$

where $a_1, a_2, \ldots, a_L$ are rationally independent real numbers[1] and each b_i is drawn independently from the constellation $C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\}$. Clearly, the real value x is a combination of L data streams, and the constellation observed at the receiver consists of $(2Q+1)^L$ signal points.

By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, [17], [18] bounded the minimum distance d_{min} of points in the receiver's constellation. Furthermore, for any $\epsilon > 0$, there exists a constant k_ϵ such that

$$d_{min} \geq \frac{k_\epsilon a}{Q^{L-1+\epsilon}} \tag{10}$$

for almost all rationally independent $\{a_i\}_{i=1}^{L}$, except 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 error probability can be made arbitrarily small, with rate $R \approx \frac{1}{2} \log P$.

Furthemore, as a simple extension, if b_i is sampled independently from different constellations $C_i(a, Q_i)$, the lower bound (10) can be modified as

$$d_{min} \geq \frac{k_\epsilon a}{(\max_i Q_i)^{L-1+\epsilon}} \tag{11}$$

IV. An Achievable Scheme

The idea behind the achievable scheme is to exploit the rational *dimensions* in the real space. Reference [18] first introduced this idea to achieve $\frac{1}{2}$ d.o.f. per transmitter-receiver pair in the interference channel. Reference [16] followed it to provide an achievable secure d.o.f. for the MISO compound wiretap channel.

If the received signal is a linear combination of multiple PAM data streams and the coefficients are rationally independent, the receiver can decode the messages with probability of error $P_e \to 0$ as $P \to \infty$. We can treat each channel coefficient as a *dimension* such that the corresponding signal transmitted along it can be decoded without error. Since the number of data streams could be any finite number, in this sense, the number of such *dimensions* in one-dimensional real space is likely countably infinitely many. Thus, by utilizing real interference alignment, we can align interference at both the legitimate receivers and the eavesdroppers.

Let $\bar{n}$ and $\bar{m}$ be two large fixed positive integers which will be specified later. Let us denote the set T as

$$T = \left\{ \left(\prod_{j=1}^{K} \prod_{i=1}^{K} h_{ji}^{r_{ji}} \right) \left(\prod_{k=1}^{N} \prod_{p=1}^{K} g_{kp}^{s_{kp}} \right) \,\middle|\, 0 \leq r_{ji} \leq \bar{n}, 0 \leq s_{kp} \leq \bar{m} \right\} \tag{12}$$

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

We assume that all of the elements in this set are rationally independent. For a K-user interference compound wiretap channel with N eavesdroppers, the probability of channel gains satisfying the above conditions is 1, i.e., for almost all the K-user interference compound wiretap channels with N eavesdroppers the corresponding set T is rationally independent. The cardinality of the set T is $(\bar{n}+1)^{K^2}(\bar{m}+1)^{NK}$.

The key idea here is to exploit the *dimensions* to align the intended data streams in half of the observed space and the interference in the other half; meanwhile, reduce the *dimension* size observed by the eavesdropper as much as possible to achieve a $\frac{1}{2} - \frac{1}{2K}$ secure d.o.f. for each transmitter-receiver pair.

For each transmitter i, choose the *dimensions* T_i

$$T_i = \left\{ \left(\prod_{j=1}^{K} \prod_{l=1}^{K} h_{jl}^{r_{jl}} \right) \left(\prod_{k=1}^{N} \prod_{p=1}^{K} g_{kp}^{s_{kp}} \right) \right\} \tag{13}$$

where $0 \leq s_{kp} < \bar{m}$ and r_{jl} satisfies the following conditions

$$\begin{cases} r_{jl} = 0, & j = l \\ 0 \leq r_{ji} \leq \bar{n} - 1, & j \neq i \\ 0 \leq r_{jl} \leq \bar{n}, & \text{otherwise} \end{cases} \tag{14}$$

Clearly, by definition, $T_i \subset T$. The cardinality of set T_i is $M_i = M = \bar{n}^{K-1}(\bar{n}+1)^{(K-1)^2}\bar{m}^{NK}$. Let $\mathbf{a}_i \in \mathcal{R}^{M_i \times 1}$ be a vector consisting of all the elements in T_i. In each channel use, let $\mathbf{u_i} \in \mathcal{R}^{M_i \times 1}$ be a vector whose elements are sampled independently and uniformly from a PAM constellation $C(a, Q)$. Then user i transmits the signal $x_i = \mathbf{a}_i^T \mathbf{u_i}$. In this way, user i transmits M_i different data streams along all *dimensions* of T_i.

For each receiver j, the intended data streams from transmitter j are in the *subspace* with *dimensions* R_j

$$R_j = h_{jj} T_j = \{h_{jj} \cdot l \,|\, l \in T_j\} \tag{15}$$

Clearly $R_j \subset T$. Now consider the interference I_{ji} due to transmitter i at receiver j. I_{ji} is in the *subspace* with *dimensions* $R_{ji} = h_{ji} T_i$. Denote by R'_j the set

$$R'_j = \left\{ \left(\prod_{q=1}^{K} \prod_{l=1}^{K} h_{ql}^{r_{ql}} \right) \left(\prod_{k=1}^{N} \prod_{p=1}^{K} g_{kp}^{s_{kp}} \right) \right\} \tag{16}$$

where $0 \leq s_{kp} < \bar{m}$, $r_{qq} = 0$ for all $q \in \{1, 2, \ldots, K\}$, and $0 \leq r_{ql} \leq \bar{n}$, otherwise. Then, based on the definition of T_i, for all $i \in \{1, 2, \ldots, K\} \backslash \{j\}$, the *dimension* set $R_{ji} = h_{ji} T_i$ of interference I_{ji} satisfies $R_{ji} \subset R'_j$, i.e., all the interference due to other transmitters is in the *subspace* with *dimensions* R'_j. The cardinality of R'_j is $M'_j = M' = (\bar{n}+1)^{K(K-1)}\bar{m}^{NK}$. Besides, since h_{jj} is not in the expression of any element in R'_j, but it is in R_j, R_j and R'_j are disjoint. Furthermore, the sizes of the *dimensions* of intended signals and interference have the following relationship

$$\lim_{\bar{n} \to \infty} \frac{M}{M + M'} = \lim_{\bar{n} \to \infty} \frac{1}{1 + \frac{(\bar{n}+1)^{K(K-1)}\bar{m}^{NK}}{\bar{n}^{K-1}(\bar{n}+1)^{(K-1)^2}\bar{m}^{NK}}} = \frac{1}{2} \tag{17}$$

i.e., when $\bar{n}$ is chosen large enough, the *space* of the signal

constellation is partitioned into two equal and disjoint halves with respect to the rational *dimension*.

For each eavesdropper k, all the observed signals due to all the transmitters are in the *subspace* with the following *dimensions*

$$E_k = \sum_{i=1}^{K} g_{ki} T_i \subset E = \left\{ \left(\prod_{j=1}^{K} \prod_{i=1}^{K} h_{ji}^{r_{ji}} \right) \left(\prod_{p=1}^{N} \prod_{q=1}^{K} g_{pq}^{s_{pq}} \right) \right\} \tag{18}$$

where $0 \leq s_{pq} \leq \bar{m}$, $r_{ii} = 0$ for all $i \in \{1, 2, \ldots, K\}$, and $0 \leq r_{ji} \leq \bar{n}$, otherwise. The cardinality of E is $(\bar{n}+1)^{K(K-1)}(\bar{m}+1)^{NK}$. As we designed, each transmitter sends M data streams along different *dimensions*, which means that all of the transmitters send a total of $K \cdot M$ data streams. However, the size of *dimensions* eavesdropper can observe is only $|E|$, where

$$\lim_{\bar{n},\bar{m}\to\infty} \frac{M}{|E|} = \lim_{\bar{n},\bar{m}\to\infty} \frac{\bar{n}^{K-1}(\bar{n}+1)^{(K-1)^2}\bar{m}^{NK}}{(\bar{n}+1)^{K(K-1)}(\bar{m}+1)^{NK}} = 1 \tag{19}$$

i.e., for large enough $\bar{n}, \bar{m}$ each eavesdropper can only decode the information along approximately M *dimensions*, which is too small to decipher the original $K \cdot M$ information streams.

V. Performance Analysis

For each transmitter-receiver pair i, the intended data streams from transmitter i observed by receiver i are in the *subspace* R_i and the interference due to other transmitters are in the *subspace* R_i'. As we mentioned in previous sections, $R_i \bigcap R_i' = \phi$ and elements in $R_i \bigcup R_i'$ are rationally independent. In each *dimension* of R_i, the data stream is sampled from a PAM $C(a, Q)$, and in each *dimension* of R_i', the combined data stream is at most sampled from a PAM $C[a, (K-1)Q]$. To reliably decode the intended data streams at receiver i, it suffices to choose

$$Q = \frac{1}{K-1} P^{\frac{1-\epsilon}{2(M_i+M_i'+\epsilon)}} = \frac{1}{K-1} P^{\frac{1-\epsilon}{2(M+M'+\epsilon)}} \tag{20}$$

and

$$a = \frac{\gamma P^{\frac{1}{2}}}{Q} \tag{21}$$

where γ is a constant independent of P. Then, the probability of error is

$$\begin{aligned} P_e &\leq \exp\left\{-\frac{d_{min}^2}{8}\right\} \\ &\leq \exp\left\{-\frac{k_\epsilon^2 \gamma^2 P}{8Q^2[(K-1)Q]^{2(M+M'-1+\epsilon)}}\right\} \\ &\leq \exp\left\{-\frac{k_\epsilon^2 \gamma^2 (K-1)^2 P}{8[(K-1)Q]^{2(M+M'+\epsilon)}}\right\} \\ &\leq \exp\left\{-\eta P^{\epsilon}\right\} \end{aligned} \tag{22}$$

where $\eta = k_\epsilon^2 \gamma^2 (K-1)^2/8 > 0$ is a constant independent of P. Then, $P_e \to 0$ as $P \to \infty$.

For each transmitter i, the channel input x_i is constructed by a deterministic function of the uniform random variable $\mathbf{u}_i$, and for all possible channel input value x_i takes, $\mathbf{u_i}$ and x_i are related through a one-to-one mapping. It is sufficient to consider a new interference network with $\{\mathbf{u}_i\}$ as channel inputs, and $\{y_j\}, \{z_k\}$ as channel outputs for the receivers and eavesdroppers, respectively.

We claim that, for each transmitter-receiver pair i, the secrecy rate

$$R_s = \min_i I(\mathbf{u}_i; y_i) - \frac{1}{K} \max_k I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k) \tag{23}$$

is achievable. We can verify this by the following arguments. By the Lemma A.1 in [14], it is sufficient to consider the enhanced eavesdroppers, each with outputs $z_k' = (z_k, \tilde{z}_k)$ such that $I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k') = \max_k I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k)$. For each secrecy codebook of transmitter-receiver pair i, we generate $2^{n(R_s+R_c)}$ n-length codewords. We independently assign each codeword to one of 2^{nR_s} bins each having 2^{nR_c} codewords. For message m_i, transmitter i chooses the corresponding bin and uniformly independently chooses a codeword denoted by $\mathbf{u}_i$ in that bin with randomization index m_i'. To satisfy the reliability and secrecy constraints, we choose R_s and R_c as follows

$$\begin{aligned} R_s &= \min_i I(\mathbf{u}_i; y_i) - \frac{1}{K} \max_k I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k) \\ R_c &= \frac{1}{K} \max_k I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k) \end{aligned} \tag{24}$$

Clearly, $R_s + R_c \leq I(\mathbf{u}_i; y_i)$, which implies that receiver i can decode m_i with small probability of error as $n \to \infty$. Next, we denote all of the messages as the vector $\mathbf{m} = [m_1, m_2, \ldots, m_K]$ and all of the randomization indices as the vector $\mathbf{m}' = [m_1', m_2', \ldots, m_K']$. Then, the equivocation rate $\frac{1}{n} H(\mathbf{m}|{z_k'}^n)$ of the enhanced eavesdropper k can be lower bounded as

$$\begin{aligned} H(\mathbf{m}|{z_k'}^n) &= H(\mathbf{m}) - I(\mathbf{m}; {z_k'}^n) \\ &= H(\mathbf{m}) - H({z_k'}^n) + H({z_k'}^n|\mathbf{m}) \\ &= H(\mathbf{m}) \\ &\quad -\big[I(\mathbf{m}, \mathbf{m}'; {z_k'}^n) + H({z_k'}^n|\mathbf{m}, \mathbf{m}')\big] \\ &\quad +\big[I(\mathbf{m}'; {z_k'}^n|\mathbf{m}) + H({z_k'}^n|\mathbf{m}, \mathbf{m}')\big] \\ &= H(\mathbf{m}) - I(\mathbf{m}, \mathbf{m}'; {z_k'}^n) + I(\mathbf{m}'; {z_k'}^n|\mathbf{m}) \\ &= H(\mathbf{m}) - I(\mathbf{m}, \mathbf{m}'; {z_k'}^n) \\ &\quad +H(\mathbf{m}'|\mathbf{m}) - H(\mathbf{m}'|\mathbf{m}, {z_k'}^n) \\ &= H(\mathbf{m}) + H(\mathbf{m}') - I(\mathbf{m}, \mathbf{m}'; {z_k'}^n) \\ &\quad -H(\mathbf{m}'|\mathbf{m}, {z_k'}^n) \end{aligned} \tag{25}$$

where $H(\mathbf{m}'|\mathbf{m}) = H(\mathbf{m}')$ follows from the fact that randomization indices are independent of bin indices. In (25), we use $H(\cdot)$ to denote both entropy and differential entropy. The second item in (25) is

$$H(\mathbf{m}') = \sum_{i=1}^{K} nR_c = nKR_c = n \max_k I(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K; z_k) \tag{26}$$

and we can bound the third item as

$$\begin{aligned} I(\mathbf{m},\mathbf{m}';{z_k'}^n) &\leq I(\mathbf{u}_1^n,\mathbf{u}_2^n,\ldots,\mathbf{u}_K^n;{z_k'}^n) \\ &\leq nI(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;z_k')+n\epsilon_1 \\ &= n\max_k I(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;z_k) \\ &\quad +n\epsilon_1 \end{aligned} \tag{27}$$

where $\epsilon_1 \to 0$ as $n \to \infty$, and $(\mathbf{m},\mathbf{m}') \to (\mathbf{u}_1^n,\mathbf{u}_2^n,\ldots,\mathbf{u}_K^n) \to {z_k'}^n$. Finally, the fourth item can be bounded as follows

$$H(\mathbf{m}'|\mathbf{m},{z_k'}^n) \leq n\epsilon_2 \tag{28}$$

where $\epsilon_2 \to 0$ as $n \to \infty$. This is because the enhanced eavesdropper k can decode randomization indices given the messages and the observation $z_k^{'n}$. Then, Fano's inequality implies (28). From (26), (27) and (28), we can write (25) as

$$\frac{1}{n}H(\mathbf{m}|{z_k'}^n) \geq \frac{1}{n}H(\mathbf{m}) - \epsilon_1 - \epsilon_2 \tag{29}$$

which implies that $\frac{1}{n}H(\mathbf{m}|z_k^n) \geq \frac{1}{n}H(\mathbf{m}|{z_k'}^n) \geq \frac{1}{n}H(\mathbf{m}) - \epsilon_1 - \epsilon_2$. This concludes our proof.

In order to calculate the achievable secrecy rate R_s in (23), we bound the mutual information $I(\mathbf{u}_i;y_i)$ and $I(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;z_k)$ separately. For transmitter-receiver pair i, $I(\mathbf{u}_i;y_i)$ can be lower bounded as

$$\begin{aligned} I(\mathbf{u}_i;y_i) &= H(\mathbf{u}_i) - H(\mathbf{u}_i|y_i) \\ &\overset{(a)}{\geq} M\log(2Q+1) - h(P_e) \\ &\quad -P_eM\log(2Q+1) \\ &\overset{(b)}{\geq} M\log(2Q+1) - 1 \\ &\quad -\exp\left(-\eta P^{\epsilon}\right)M\log(2Q+1) \\ &\overset{(c)}{\geq} M\log\left[\frac{2}{K-1}P^{\frac{1-\epsilon}{2(M+M'+\epsilon)}}+1\right]-1 \\ &\quad -\exp\left(-\eta P^{\epsilon}\right)M\log(2Q+1) \\ &\geq \frac{M(1-\epsilon)}{2(M+M'+\epsilon)}\log P + o(\log P) \end{aligned} \tag{30}$$

where in (a) $\mathbf{u}_i$ is a random vector drawn uniformly from $(2Q+1)^M$ points and $H(\mathbf{u}_i|y_i)$ is upper bounded by Fano's inequality, in (b) the binary entropy $h(P_e)$ is upper bounded by 1 and (22) is substituted for P_e, in (c) (20) is substituted for Q, and the o functions are the little-o functions.

Next, we upper bound $I(\mathbf{u}_i;z_k)$. For each eavesdropper k, we know that the data streams from each transmitter are transmitted along different *dimensions*, and the total $K\cdot M = K\bar{n}^{K-1}(\bar{n}+1)^{(K-1)^2}\bar{m}^{NK}$ data streams are distributed in the $|E| = (\bar{n}+1)^{K(K-1)}(\bar{m}+1)^{NK}$ *dimensions*. This implies that, in each *dimension* observed by eavesdropper k, there are at most K independent data streams constituting a $C(a,KQ)$ PAM constellation, i.e.,

$$z_k = \sum_{i=1}^{K} g_{ki}x_i + w_k = \sum_{i=1}^{K} g_{ki}\mathbf{a}_i^T\mathbf{u_i} + w_k = \sum_{l\in E} l\cdot\tilde{u}_l + w_k \tag{31}$$

where l denotes each *dimension* in E and $\tilde{u}_l$ is the signal observed in this *dimension*.

Even if we assume that the eavesdropper can decode the signal in each *dimension* correctly, it cannot distinguish the multiple combined data streams in the $C(a,KQ)$ constellation. Therefore, for each eavesdropper k

$$\begin{aligned} I(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;z_k) &\overset{(a)}{\leq} I\big(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;\sum_{l\in E} l\cdot\tilde{u}_l\big) \\ &\leq H\big(\sum_{l\in E} l\cdot\tilde{u}_l\big) \\ &\overset{(b)}{\leq} \sum_{l\in E} H(\tilde{u}_l) \end{aligned} \tag{32}$$

where in (a) follows $(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K) \to \sum_{l\in E} l\cdot\tilde{u}_l \to z_k$, (b) follows from the inequality $H(X+Y) \leq H(X,Y) = H(X)+H(Y|X) \leq H(X)+H(Y)$. Furthermore, each $\tilde{u}_l$ is sampled independently, but not uniformly, from a PAM $C(a,KQ)$. Hence $H(\tilde{u}_l) \leq \log(2KQ+1)$, and

$$\begin{aligned} I(\mathbf{u}_1,\ldots,\mathbf{u}_K;z_k) &\leq |E|\log(2KQ+1) \\ &= |E|\log\left(\frac{2K}{K-1}P^{\frac{1-\epsilon}{2(M+M'+\epsilon)}}+1\right) \\ &\leq \frac{1-\epsilon}{2}\cdot\frac{|E|}{(M+M'+\epsilon)}\log P \\ &\quad +o(\log P) \\ &= \frac{1-\epsilon}{2}\left[\frac{M}{M+M'+\epsilon}+\epsilon_{\bar{n},\bar{m}}\right]\log P \\ &\quad +o(\log P) \end{aligned} \tag{33}$$

where in the last equality we use the the result of (19), and $\epsilon_{\bar{n},\bar{m}} \to 0$ as $\bar{n},\bar{m} \to \infty$.

From (30) and (33), we can derive the lower bound of R_s in (23) as

$$\begin{aligned} R_s &= \min_i I(\mathbf{u}_i;y_i) - \frac{1}{K}\max_k I(\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_K;z_k) \\ &\geq \frac{M(1-\epsilon)}{2(M+M'+\epsilon)}\log P \\ &\quad -\frac{1-\epsilon}{2K}\left[\frac{M}{M+M'+\epsilon}+\epsilon_{\bar{n},\bar{m}}\right]\log P + o(\log P) \\ &= \left[\frac{M(1-\epsilon)}{2(M+M'+\epsilon)}\left(1-\frac{1}{K}\right)\log P\right] \\ &\quad -\epsilon_{\bar{n},\bar{m}}\frac{1-\epsilon}{2K}\log P + o(\log P) \end{aligned} \tag{34}$$

If we choose $\bar{n},\bar{m}$ sufficiently large and ϵ small enough, as shown in (17), the lower bound (34) can approach $(\frac{1}{2}-\frac{1}{2K})\log P + o(\log P)$. This proves our claim in Section II.

VI. Conclusions

For the K-user interference channel, [19] has shown that the degrees of freedom (d.o.f.) capacity of each transmitter-receiver pair is $\frac{1}{2}$. When there are eavesdroppers in this interference network, the achievable secure d.o.f. proposed in this paper is lower than $\frac{1}{2}$, but still remains a constant value $\frac{1}{2}-\frac{1}{2K}$, as we keep adding eavesdroppers. Although the achievable scheme involves the number N of eavesdroppers,

as far as N is finite, the result is independent of N. To the best of our knowledge, $\frac{1}{2}$ is the only upper bound in our case also, and the gap of $\frac{1}{2K}$ remains.

The idea behind our achievable scheme is to exploit the real interference alignment technique introduced in [17], [18]. The key to achieve a non-vanishing secure d.o.f. is to employ interference alignment at both the receivers and the eavesdroppers at the same time. Due to the existence of eavesdroppers, there is a $\frac{1}{2K}$ d.o.f. penalty. This is needed to satisfy the secrecy constraints.

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

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

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

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

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.

[7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channe," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," submitted to *IEEE Trans. Inf. Theory*, Oct. 2007. Also available at [arXiv:0710.1920].

[10] T. Liu and S. S. (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[11] 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.

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

[13] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, to appear. Also available at [arXiv:0903.3096].

[14] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, Dec. 2008.

[15] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," submitted to *IEEE Trans. Inf. Theory*, Oct. 2009. Also available at [arXiv:0910.3033].

[16] A. Khisti, "Interference alignment for the multi-antenna compound wiretap channel," submitted to *IEEE Trans. Inf. Theory*, Mar. 2010. Also available at [arXiv:1002.4548].

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

[18] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," submitted to *IEEE Trans. Inf. Theory*, Nov. 2009. Also available at [arXiv:0908.2282].

[19] 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, 2008.

[20] B. Nazer, S. A. Jafar, M. Gastpar, and S. Vishwanath, "Ergodic interference alignment," *IEEE International Symposium on Information Theory*, 2009.

[21] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, Aug. 2008.

[22] R. Etkin and E. Ordentlich, "On the Degrees-of-Freedom of the K-user Gaussian interference channel," submitted to *IEEE Trans. Inf. Theory*, Jun. 2008. Also available at [arXiv:0901.1695].

[23] T. Gao and S. A. Jafar, "On the secure Degrees of Freedom of wireless X networks," *In 46th Annual Allerton Conference on Communication, Control and Computing, UIUC, IL*, pp. 826–833, Sept. 2008.

[24] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," submitted to *IEEE Trans. Inf. Theory*, Oct. 2008. Also available at [arXiv:0810.1187].

[25] ——, "On the secure Degrees of Freedom in the K-user Gaussian interference channel," *IEEE International Symposium on Information Theory*, 2008.

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

[27] ——, "Providing secrecy with structured codes: Tools and applications to two-user gaussian channels," submitted to *IEEE Trans. Inf. Theory*, Jul. 2009. Also available at [arXiv:0907.5388].

[28] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure Degrees-of-Freedom of the multiple-access-channel," submitted to *IEEE International Symposium on Information Theory* 2010. Also available at [arXiv:1003.0729].