

On the MISO Compound Wiretap Channel

Ashish Khisti
ECE Dept.
University of Toronto
Toronto, ON, M1B 5P1
akhisti@comm.utoronto.ca

Abstract—We study the secure degrees of freedom (d.o.f.) of the MISO compound wiretap channel. The transmitter has M antennas, whereas the legitimate receiver and the eavesdropper each have one antenna and the channel vectors take one of finitely many values. If the number of states of either the legitimate receiver or the eavesdropper channel is less than M , then we achieve full 1 d.o.f. If however the number of states of both the legitimate receiver and the eavesdropper channel are at-least equal to M , then we establish that the d.o.f. is strictly less than 1. Our upper bound is, to our knowledge, the first bound which is strictly tighter than the “pairwise upper bound”. Lower bounds that combine ideas based on time-sharing, noise transmission, signal alignment and multi-level coding schemes are also provided.

I. INTRODUCTION

The wiretap channel, introduced in [1] is an information theoretic model for secure communications at the physical layer. In this model, there are three terminals — a sender, a receiver and an eavesdropper. A wiretap code simultaneously ensures reliable communication to the legitimate receiver and secrecy with respect to the eavesdropper. In recent times that has been a significant interest in applying this model to wireless communication systems. Some recent works include secure communications over fading channels [2]–[4], multi-antenna wiretap channels [5]–[13] and several multiuser channels.

The wiretap channel model assumes that the eavesdropper’s channel statistics are known to all the terminals. As one justification, when the receiver channels are degraded, the wiretap code can be designed for the worst-case eavesdropper in a class. However in many cases of practical interest, such as in the case of multi-antenna channels, the receivers cannot be ordered in this fashion and it is not possible to characterize the worst-case eavesdropper.

A model that incorporates the lack of knowledge of the receiver channels is a compound extension of the wiretap channel. In the model studied in [14] the channels of the legitimate receiver and the eavesdropper take one of finitely many values. The problem is equivalent to broadcasting a common message to multiple intended receivers while keeping the message secure against a collection of non-colluding eavesdroppers. A lower bound on the secrecy capacity is established which amounts to sending information at a rate such that that the worst legitimate receiver can decode while every eavesdropper channel remains in

(asymptotically) perfect equivocation. One immediate upper bound to capacity is the *pairwise upper bound*. This bound essentially (c.f. (51)) considers all possible receiver-eavesdropper pairs and selects the pair with smallest capacity assuming all other receivers are absent. This bound coincides with the coding scheme in [14] when the underlying channels are deterministic and the legitimate receiver has only one realization. The pairwise upper bound is also tight for parallel reversely degraded wiretap channels when there is one legitimate receiver and multiple eavesdroppers [3], [15] or when there are multiple receivers and one eavesdropper [2]. Other recent works on the compound wiretap channel include [16], [17].

To the best of our knowledge, no upper bounds besides the pairwise upper bound are known for the compound wiretap channel. All the conclusive capacity results previously used the pairwise upper bound in the converse and proposed coding schemes that attain it. In this paper we study the multi-input-single-output (MISO) wiretap channel, where both the legitimate receivers and the eavesdroppers channel take one of finitely many values. We develop a new upper bound on secrecy-rate that is tighter than the pairwise upper bound and establishes that there is a loss in degrees of freedom due to uncertainty of channel state information at the transmitter. In addition we provide lower bounds based on time-sharing and noise transmission strategies and show that in some special cases these bounds can be further improved using signal alignment and multi-level coding strategies. While our analysis is restricted to the MISO wiretap channel, we expect techniques developed in deriving upper and lower bounds to be applicable to related problems such as the compound extension of the MIMO wiretap channel, the two receiver broadcast channel with mutually confidential messages [9] and the multi-receiver broadcast channel with an external wiretapper [12], [13]. We note that recently signal and interference alignment schemes have been used in the wiretap channel literature in e.g. [18]–[20]. Secure degrees of freedom for the compound wiretap channel are studied previously in [14]. The expressions involve optimizing over certain subspaces defined by the channel vectors and do not take into account techniques such as time-sharing, signal alignment or multi-level coding.

In the remainder of the paper, section II introduces the channel model, section III considers the cases

when there is no loss in degrees of freedom due to channel uncertainty, section IV provides lower bounds on achievable degrees of freedom whereas section V establishes an upper bound on the secure degrees of freedom.

II. CHANNEL MODEL

The model includes one transmitter with M antennas, one receiver and one eavesdropper, each with one antenna. The channels of the legitimate receiver and the eavesdropper are given by,

$$\begin{aligned} y(t) &= \mathbf{h}^T \mathbf{x}(t) + v(t) \\ z(t) &= \mathbf{g}^T \mathbf{x}(t) + w(t) \end{aligned} \quad t = 1, 2, \dots, n. \quad (1)$$

where t denotes the time index, y and z denote the channel output symbols at the legitimate receiver and the eavesdropper respectively whereas $\mathbf{h}, \mathbf{g} \in \mathbb{R}^M$ denote the corresponding channel matrices of the legitimate receiver and the eavesdropper respectively. The additive noise variables are independent (across users and time) and Gaussian with zero mean and unit variance. We assume an average power constraint on the input i.e., $E[\sum_{t=1}^n \|\mathbf{x}(t)\|^2] \leq P$, where $\|\cdot\|$ denotes the standard Euclidean norm.

We further assume that the channels matrices of the legitimate receiver and the eavesdropper belong of a finite set i.e.,

$$\begin{aligned} \mathbf{h} \in \mathcal{H} &= \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_{J_r}\} \\ \mathbf{g} \in \mathcal{G} &= \{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{J_e}\} \end{aligned} \quad (2)$$

Unless we explicitly state otherwise, we assume that \mathcal{H} and \mathcal{G} are such that any combination of M vectors taken from either of the sets are linearly independent. This assumption is satisfied for example if the channel vectors are sampled from any continuous distribution. The actual realization of \mathbf{h} and \mathbf{g} is known to the respective receivers whereas only the sets \mathcal{H} and \mathcal{G} are known to the remaining terminals. We use the notation y_j to denote the output at the receiver when $\mathbf{h} = \mathbf{h}_j$ for $j = 1, 2, \dots, J_r$. Similarly the notation z_j denotes the output at the eavesdropper when $\mathbf{g} = \mathbf{g}_j$ for $j = 1, 2, \dots, J_e$. Note that the compound wiretap channel is equivalent to another scenario where there are a total of J_r legitimate receivers, each interested in a common message and J_e non-colluding eavesdroppers. The channel output of the j th legitimate receiver is denoted by y_j while that of the j th eavesdropper is denoted by z_j . We often use the term *user* to denote a particular state of the receiver.

We will also use the notation where the transmit vectors and received symbols are concatenated together i.e., $X = [\mathbf{x}(1), \dots, \mathbf{x}(n)]$ and likewise $\mathbf{y}_j = [y_j(1), \dots, y_j(n)]$, $\mathbf{z}_k = [z_k(1), \dots, z_k(n)]$ etc. In this notation the channel (1) can be expressed as

$$\begin{aligned} \mathbf{y}_j &= \mathbf{h}_j^T X + \mathbf{v}_j, & j &= 1, \dots, J_r \\ \mathbf{z}_k &= \mathbf{g}_k^T X + \mathbf{w}_j, & k &= 1, \dots, J_e \end{aligned} \quad (3)$$

A compound wiretap encoder maps a message m , uniformly distributed over a set of size 2^{nR} , to the channel input sequence \mathbf{x}^n . The decoder produces a message estimate $\hat{m}_j = g_j(y_j^n; \mathbf{h}_j)$. A rate R is achievable if there exist a sequence of encoder and decoders of such that $\Pr(m \neq \hat{m}_j) \rightarrow 0$ as $n \rightarrow \infty$ for each $j = 1, 2, \dots, J_r$ and $\frac{1}{n} I(m; z_j^n) \rightarrow 0$ for each $j = 1, 2, \dots, J_e$. The largest rate achievable under these constraints is the *compound secrecy capacity*. Of particular interest is the degrees of freedom (d.o.f.) of the compound wiretap channel. We say that d d.o.f. are achievable on the compound wiretap channel, if there exists a sequence of achievable rates $R(P)$, indexed by power P , such that

$$d = \lim_{P \rightarrow \infty} \frac{R(P)}{\frac{1}{2} \log_2 P}. \quad (4)$$

The maximum attainable value of d is the *secrecy d.o.f.* of the compound wiretap channel.

III. CASES WHEN $d = 1$

It is clear that even in absence of secrecy constraints we can at-most attain 1 d.o.f. In this section we observe that when $\min(J_r, J_e) \leq 1$, it is indeed possible to attain 1 d.o.f. We first consider the case when $J_r \leq M$

Proposition 1: When $J_r < M$ the compound MISO wiretap channel achieves full 1 degree of freedom.

Proof: When the number of legitimate receiver channel states is less than M the matrix $H_r = [\mathbf{h}_1, \dots, \mathbf{h}_{J_r}]$ is a low rank matrix. We can construct $A \in \mathbb{R}^{M-J_r \times M}$ whose rows are mutually orthogonal as well as orthogonal to the columns of H_r i.e., $A \cdot H_r = 0$. Furthermore, since every eavesdropper channel state \mathbf{g}_j is linearly independent of the columns of H_r , we have that $A \mathbf{g}_j \neq 0$, since the rank of $[\mathbf{h}_1, \dots, \mathbf{h}_{J_r}, \mathbf{g}_j]$ exceeds J_r . As described below, by transmitting noise symbols along the rows of the A matrix we can thus ensure that the legitimate receiver's mutual information scales as $\frac{1}{2} \log_2 P$ while the eavesdropper's mutual information does not increase at this rate.

Let \mathbf{u} be any unit norm vector such that $\mathbf{h}_i^T \mathbf{u} \neq 0$ for $i = 1, 2, \dots, J_r$. The transmitted vector is:

$$\mathbf{x} = \mathbf{u}s + A^T \mathbf{n}, \quad (5)$$

where $s \sim \mathcal{N}(0, P_0)$ is the information bearing symbol, where $\mathbf{n} \sim \mathcal{N}(0, P_0 \mathbf{I}_{M-J_r})$ is a vector of noise symbols transmitted in the common null-space of user matrices and where $P_0 = \frac{P}{M}$ is selected to meet the transmit power constraint. Accordingly the received signals can be expressed as,

$$y_i = \mathbf{h}_i^T \mathbf{x} + v_i \quad (6)$$

$$= \mathbf{h}_i^T \mathbf{u}s + v_i, \quad (7)$$

and

$$z_j = \mathbf{g}_j^T \mathbf{x} + w_j, \quad (8)$$

$$= \mathbf{g}_j^T \mathbf{u}s + \mathbf{g}_j^T A^T \mathbf{n} + w_j. \quad (9)$$

An achievable secrecy rate is given by [14]

$$R = \min_i I(s; y_i) - \max_j I(s; z_j) \quad (10)$$

$$= \min_i \frac{1}{2} \log(1 + P_0 |\mathbf{h}_i^T \mathbf{u}|^2) - \max_j \frac{1}{2} \log \left(1 + \frac{P_0 |\mathbf{g}_j^T \mathbf{u}|^2}{1 + P_0 \|\mathbf{A} \mathbf{g}_j\|^2} \right), \quad (11)$$

which scales like $\frac{1}{2} \log P$ since $\|\mathbf{A} \mathbf{g}_j\| > 0$ for each $j = 1, 2, \dots, J_e$ and $\mathbf{h}_i^T \mathbf{u} > 0$ for $i = 1, \dots, J_r$. ■

When there are fewer than M eavesdropping channels and an arbitrary number of legitimate receiver channels we still achieve one d.o.f. by transmitting information in the common null-space of the eavesdropper channels.

Proposition 2: When $J_e < M$ the compound MISO wiretap channel achieves 1 d.o.f.

Proof: The matrix $G = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{J_e}] \in \mathbb{R}^{M \times J_e}$ is a low-rank matrix when $J_e < M$ hence we construct a matrix $B \in \mathbb{R}^{M - J_e \times M}$ with orthogonal rows such that $B \cdot G = 0$. Further because each \mathbf{h}_i is linearly independent of the columns of G , it must have a component in the null space i.e., $B \mathbf{h}_i \neq 0$ for $i = 1, \dots, J_r$. The transmitted vector is

$$\mathbf{x} = B^T \mathbf{m}, \quad (12)$$

where the information vector $\mathbf{m} \sim \mathcal{N}(0, P_1 \mathbf{I})$ is a vector of i.i.d Gaussian symbols and $P_1 = \frac{P}{M}$. Since any information transmitted along rows of B will not be seen by any eavesdropper, the resulting achievable rate is:

$$R = \min_i I(\mathbf{m}; y_i) \quad (13)$$

$$= \min_i \frac{1}{2} \log(1 + P_1 \|B \mathbf{h}_i\|^2) \quad (14)$$

which scales as $\frac{1}{2} \log P$ as $B \mathbf{h}_i \neq 0$ for each $i = 1, 2, \dots, J_r$. ■

IV. LOWER BOUNDS: $\min(J_r, J_e) \geq M$

The lower bound in Prop. 3 is based on selecting a subset of receivers to serve or a subset of eavesdroppers to hide the message against and time-sharing between the choice of these subsets. It extends the techniques in Prop. 1 and Prop. 2 to the case when $\min(J_r, J_e) \geq M$.

Proposition 3: The following degrees of freedom are achievable for the compound MISO wiretap channel when $\min(J_r, J_e) \geq M$:

$$d = \frac{M - 1}{\min(J_r, J_e)}. \quad (15)$$

Proof: We first sketch how one achieves $\frac{M-1}{J_r}$ degrees of freedom by time-sharing across the set of receivers.

1) Let $T = \binom{J_r - 1}{M - 1}$ denote all possible subsets of users of size $M - 1$. We label these subsets as

$\mathcal{S}_1, \dots, \mathcal{S}_T$. Note that each user belongs to $T_0 = \binom{J_r - 1}{M - 2}$ subsets.

2) Let n be a sufficiently large integer. A message m consists of nT_0R_0 information bits where

$$R_0 = \frac{1}{2} \log_2 P - \Theta, \quad (16)$$

and where Θ is a sufficiently large constant, (which will be specified later) that does not grow with P . The message is mapped into a codeword of a (T, T_0) erasure code \mathcal{C} i.e., $m \rightarrow (m_1, m_2, \dots, m_T)$ where each symbol m_i consists of nR_0 information bits. Each receiver retrieves the message m provided it observes any T_0 symbols. Furthermore as established in [2] suitable inner code constructions exist such that provided each of the T symbols are individually protected, the overall message remains protected. i.e.,

$$I(m_t; \mathbf{z}) \leq n\varepsilon_n, \forall t = 1, \dots, T \Rightarrow I(m; \mathbf{z}) \leq Tn\varepsilon_n \quad (17)$$

The overall rate $R = \frac{T_0}{T} R_0$ results in the following degrees of freedom:

$$d = \frac{T_0}{T} = \frac{\binom{J_r - 1}{M - 2}}{\binom{J_r}{M - 1}} = \frac{M - 1}{J_r}$$

as required.

It remains to show how to transmit message m_t such that each user in a subset \mathcal{S}_t decodes it with high probability while satisfying $I(m_t; \mathbf{z}_j) \leq n\varepsilon_n$.

3) Each subset \mathcal{S}_t is served over n channel uses. The message m_t is transmitted to $M - 1$ users belonging to this subset along the lines of Prop. 1 i.e., by transmitting information symbols in the common range space and noise in the common null space of these users (c.f. (5))

$$\mathbf{x}_t = \mathbf{u}_t s + \mathbf{a}_t n, \quad (18)$$

where \mathbf{a}_t and \mathbf{u}_t are unit norm vectors such that $\mathbf{h}_i^T \mathbf{u}_t \neq 0$ and $\mathbf{h}_i^T \mathbf{a}_t = 0$ for each $i \in \mathcal{S}_t$ and s and n are information bearing and noise symbols respectively.

Following the analysis leading to (11) we can see that the following rate is achievable:

$$R_t = \frac{1}{2} \log P - \Theta_t, \quad \Theta_t = - \min_{i \in \mathcal{S}_t} \frac{1}{2} \log |\mathbf{h}_i^T \mathbf{u}_t|^2 + \max_{j \in J_r} \frac{1}{2} \log \left(1 + \frac{|\mathbf{g}_j^T \mathbf{u}_t|^2}{|\mathbf{a}_t^T \mathbf{g}_j|^2} \right), \quad (19)$$

where Θ_t is a constant that does not scale with P . Furthermore we let Θ in (16) to be

$$\Theta = \max_t \Theta_t. \quad (20)$$

- 4) With the choice of rate in (16) every user in each subset \mathcal{S}_t can decode the message m_t with high probability. Each user will have access to T_0 elements of the codeword (m_1, \dots, m_T) and hence recover the original message m . Furthermore from the analysis in Prop. 1 it follows that for $j = 1, 2, \dots, J_r$ and each $t = 1, \dots, T$

$$I(m_t; \mathbf{z}_j) \leq n\varepsilon_n \quad (21)$$

and hence from (17) it follows that $I(m; \mathbf{z}_j) \leq nT\varepsilon_n$. Since ε_n can be made sufficiently small, the secrecy condition is satisfied.

By time-sharing with respect to the eavesdroppers the one can attain $\frac{M-1}{J_e}$ degrees of freedom as sketched below.

- 1) We consider all possible $T^e = \binom{J_e}{M-1}$ subsets of $M-1$ eavesdroppers and label them as $\mathcal{S}_1^e, \dots, \mathcal{S}_{T^e}^e$. Note that each eavesdropper belongs to a total of $T_1^e = \binom{J_e-1}{M-2}$ subsets.
- 2) Consider a parallel noise-less wiretap channel consisting of T^e links, where each link supports a rate nR_1 , where

$$R_1 = \frac{1}{2} \log P - \Omega \quad (22)$$

and Ω is a sufficiently large constant that will be specified later. Each eavesdropper is absent on a total of T_1^e links while each legitimate receiver observes all the T^e links. Following the scheme in [2] we can transmit a message m of rate $nR_1 T_1^e$ by mapping the message $m \rightarrow (m_1, \dots, m_{T^e})$. The symbol m_k , consists of nR_1 bits and forms the input message on channel k .

- 3) For each choice of \mathcal{S}_t^e , we transmit information in the common null-space of the eavesdroppers in this selected set. Let \mathbf{b}_t be a vector such that $\mathbf{b}_t^T \mathbf{g}_j = 0$ for each $j \in \mathcal{S}_t^e$ and transmit

$$\mathbf{x}_t = \mathbf{b}_t s,$$

where s is the information bearing symbol. Since each vector \mathbf{h}_i is linearly independent of any collection of $M-1$ eavesdropper channel vectors it follows that $\mathbf{h}_i^T \mathbf{b}_t \neq 0$, and one can achieve a rate

$$R_1 = \frac{1}{2} \log \left(1 + \min_{\substack{t \in \{1, \dots, T^e\} \\ i \in \{1, \dots, J_r\}}} |\mathbf{h}_i^T \mathbf{b}_t|^2 P \right) \geq \frac{1}{2} \log P - \Omega, \quad (23)$$

where

$$\Omega = - \min_{\substack{t \in \{1, \dots, T^e\} \\ i \in \{1, \dots, J_r\}}} \frac{1}{2} \log |\mathbf{h}_i^T \mathbf{b}_t|^2. \quad (24)$$

With this choice of Ω , each receiver decodes each of the messages m_1, \dots, m_T with high probability. Furthermore, each of the eavesdropper does

not have access to T_1 sub-messages corresponding to the subsets \mathcal{S}_t to which it belongs. By virtue of our code construction, this ensures that $I(m; \mathbf{z}_j) \leq n\varepsilon_n$.

The overall achievable rate is given by $R = \frac{T_1^e}{T^e} R_1$ and hence the achievable degrees of freedom are given by

$$d = \frac{T_1^e}{T^e} = \frac{\binom{J_e-1}{M-2}}{\binom{J_e}{M-1}} = \frac{M-1}{J_e}$$

as required. \blacksquare

The time-sharing schemes in Prop. 3 can be further improved using a variety of signal alignment schemes. In our results below we assume that all the channel in (1) are drawn by sampling a continuous distribution and remain fixed thereafter.

1) Signal Alignment:

Proposition 4: Consider a compound MISO wiretap channel with $M = 2$ transmit antennas and $J_r = 3$ states and $J_e \geq 3$. By aligning the signals of legitimate receivers in a lower dimensional subspace, one can achieve up to 1/2 degrees of freedom (almost surely).

Remark 1: We note that the time-sharing approach in Prop. 3 achieves 1/3 d.o.f Thus the signal alignment scheme can strictly improve the secrecy rate.

Proof: The suggested scheme involves coding over an extension of two symbols. The channel matrices over this extension are given by

$$H_i = \begin{bmatrix} \mathbf{h}_i^T & \mathbf{0} \\ \mathbf{0} & \mathbf{h}_i^T \end{bmatrix}, \quad G_j = \begin{bmatrix} \mathbf{g}_j^T & \mathbf{0} \\ \mathbf{0} & \mathbf{g}_j^T \end{bmatrix} \quad (25)$$

and the corresponding received symbols, taken two at a time, are expressed as

$$\mathbf{y}_i = H_i \mathbf{x} + \mathbf{v}_i, \quad \mathbf{z}_j = G_j \mathbf{x} + \mathbf{w}_j \quad (26)$$

where \mathbf{y}_i and \mathbf{z}_j are length-two received vectors at the legitimate receiver and the eavesdropper respectively, the input $\mathbf{x} \in \mathbb{R}^4$ is a length four vector and \mathbf{v}_i and \mathbf{w}_j are length-two noise vectors. The basic idea is to force each receiver to receive signal in a one dimensional subspace by post multiplying the received symbols with a length 2 vector i.e.,

$$\tilde{y}_i = \mathbf{r}_i^T H_i \mathbf{x} + \mathbf{r}_i^T \mathbf{v}_i$$

Signal alignment is used to select the vectors $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$ in such a way that

$$\mathbf{r}_3^T H_3 \in \text{span}(\mathbf{r}_1^T H_1, \mathbf{r}_2^T H_2). \quad (27)$$

This can be accomplished for example by letting \mathbf{r}_3 to be an arbitrary length 2 vector and selecting \mathbf{r}_1 and \mathbf{r}_2 as follows:

$$[\mathbf{r}_1^T \quad \mathbf{r}_2^T] = \mathbf{r}_3^T H_3 \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}^{-1}. \quad (28)$$

By virtue of (27) we have that

$$\text{rank} \left(\tilde{H} = \begin{bmatrix} \mathbf{r}_1^T H_1 \\ \mathbf{r}_2^T H_2 \\ \mathbf{r}_3^T H_3 \end{bmatrix} \right) = 2 \quad (29)$$

and hence there exist a two dimensional space defined by the matrix $B \in \mathbb{R}^{4 \times 2}$ such that $\tilde{H} \cdot B = 0$. The proposed scheme sends noise along this subspace. Since the channel vectors \mathbf{g}_j are sampled independently of \mathbf{h}_i , we have that almost surely

$$\text{rank}(G_j \cdot B) = \text{rank} \begin{pmatrix} \mathbf{g}_j^T \mathbf{b}_1^1 & \mathbf{g}_j^T \mathbf{b}_2^1 \\ \mathbf{g}_j^T \mathbf{b}_1^2 & \mathbf{g}_j^T \mathbf{b}_2^2 \end{pmatrix} = 2 \quad (30)$$

where we have introduced

$$B = \begin{bmatrix} \mathbf{b}_1^1 & \mathbf{b}_2^1 \\ \mathbf{b}_1^2 & \mathbf{b}_2^2 \end{bmatrix}.$$

Furthermore, let \mathbf{t} be a vector such that $\mathbf{r}_i^T H_i \mathbf{t} \neq 0$ then the transmitted vector is of the form:

$$\mathbf{x} = \mathbf{t}s + B\mathbf{n}, \quad (31)$$

where $s \sim \mathcal{N}(0, \frac{P}{3})$ is the information bearing symbol whereas $\mathbf{n} \sim \mathcal{N}(0, \frac{P}{3} \mathbf{I}_2)$ is a vector of noise symbols. The received symbols at the legitimate receivers and the eavesdroppers are given as:

$$\begin{aligned} \tilde{y}_i &= \mathbf{r}_i^T H_i \mathbf{t}s + \mathbf{r}_i^T \mathbf{v}_i \\ \mathbf{z}_j &= G_j \mathbf{t}s + G_j B\mathbf{n} + \mathbf{w} \end{aligned} \quad (32)$$

An achievable rate for the compound wiretap channel is [14]

$$R = \frac{1}{2} \left(\min_i I(s; y_i) - \max_j I(s; \mathbf{z}_j) \right) \quad (33)$$

where the factor of 1/2 appears because we are aggregating two symbols to send each information symbol. Our claim is complete once we show that

$$I(s; y_j) = \frac{1}{2} \log P + \Theta(1) \quad (34)$$

$$I(s; \mathbf{z}_j) = \Theta(1) \quad (35)$$

To establish (34) note that

$$\begin{aligned} I(s; y_i) &= h(y_i) - h(y_i|s) \\ &= \frac{1}{2} \log \left(1 + \frac{P}{3} \frac{|\mathbf{r}_i^T H_i \mathbf{t}|^2}{\|\mathbf{r}_i\|^2} \right) \end{aligned}$$

from which (34) follows since by construction $\mathbf{r}_i^T H_i \mathbf{t} \neq 0$. To establish (35) note that

$$\begin{aligned} I(s; \mathbf{z}_j) &= h(\mathbf{z}_j) - h(\mathbf{z}_j|s) \\ &= \frac{1}{2} \log \det \left(I + \frac{P}{3} G_j \mathbf{t} \mathbf{t}^\dagger G_j^\dagger + \frac{P}{3} G_j B B^\dagger G_j^\dagger \right) \\ &\quad - \frac{1}{2} \log \det \left(I + \frac{P}{3} G_j B B^\dagger G_j^\dagger \right) \end{aligned} \quad (36)$$

$$= \frac{1}{2} \log \left(1 + \frac{P}{3} \mathbf{t}^\dagger G_j^\dagger \left(I + \frac{P}{3} G_j B B^\dagger G_j^\dagger \right)^{-1} G_j \mathbf{t} \right) \quad (37)$$

To show that (37) does not scale with P , we let $G_j B = U_j \Lambda_j V_j^\dagger$ be the singular value decomposition of $G_j B$ where U_j and V_j are unitary matrices and Λ_j is a 2×2 diagonal matrix. Since $G_j B$ is full rank

(c.f. (30)), it follows that both the diagonal elements of Λ_j are non-zero. Substituting in (37) we have that

$$I(s; \mathbf{z}_j) = \frac{1}{2} \log \left(1 + \frac{P}{3} \mathbf{t}^\dagger G_j^\dagger U_j^\dagger \left(I + \frac{P}{3} \Lambda_j \Lambda_j^\dagger \right)^{-1} U_j^\dagger G_j \mathbf{t} \right) \quad (38)$$

$$= \sum_{c=1}^2 \frac{1}{2} \log \left(1 + \frac{P t_c^2}{3 + P \lambda_c^2} \right) \quad (39)$$

where we introduce $\mathbf{t}^\dagger G_j^\dagger U_j^\dagger = [t_1, t_2]$. Since $\lambda_c > 0$, this shows that $I(s; \mathbf{z}_j) = \Theta(1)$ as required. ■

2) *Multi-level coding* : In the previous section we observed how one can leverage on interference alignment to improve the achievable degrees of freedom compared to time-sharing. In the following section we show how another technique, multi-level coding can also improve achievable degrees of freedom. We will restrict our attention to a specific example where $\mathbf{h}_1 = [1, 1]^\dagger$, $\mathbf{h}_2 = [1, -1]^\dagger$, $\mathbf{g}_1 = [1, 0]^\dagger$ and $\mathbf{g}_2 = [0, 1]^\dagger$.

To get insights into the multi-level coding scheme, we first consider a simple example of deterministic channels over \mathbb{F}_3 .

Proposition 5: Consider a linear deterministic channel over \mathbb{F}_3 with two input symbols x_1 and x_2 and with output symbols described as follows:

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_1 - x_2 \\ z_i &= x_i, \quad i = 1, 2 \end{aligned} \quad (40)$$

where the addition and subtraction is defined over the group in \mathbb{F}_3 . Then we can achieve a secrecy rate of $R = 1$ b/s for this channel.

Remark 2: We note that a time-sharing based rate, analogous to Prop. 3, achieves a rate of $\frac{1}{2} \log_2 3 = 0.792$ b/s. Thus the proposed rate is significantly higher than time-sharing. In the Gaussian example, a natural extension of this scheme yields significantly higher degrees of freedom than time-sharing.

Proof: The key idea behind the proof is to enable the legitimate receivers to take advantage of the field \mathbb{F}_3 in decoding while we limit the observation of the eavesdroppers to binary valued symbols. The wiretap code is illustrated below:

msg.	(x_1, x_2)
0	$(0, 0), (1, 1)$
1	$(0, 1), (1, 0)$

(41)

When message bit 0 needs to be transmitted the sender selects one of the two tuples $(0, 0)$ and $(1, 1)$ at random and transmit the corresponding value of (x_1, x_2) . Likewise when bit 1 needs to be transmitted one of the two tuples $(0, 1)$ and $(1, 0)$ will be transmitted. Note that when $b = 0$ is transmitted $y_1 \in \{0, 2\}$ while $y_2 = 0$ whereas when $b = 1$ we have that $y_1 = 1$ and $y_2 \in \{1, 2\}$. It can be readily verified that each receiver is able to recover either message. Assuming that the messages are equally likely, it can also be readily verified that the message bit is independent of

both x_1 and x_2 and thus the secrecy condition w.r.t. each eavesdropper is satisfied. ■

To generalize the above coding scheme to the Gaussian case we consider a natural multi-level extension. Fix integers T and M with the following properties: T is the smallest integer such that for a given $\varepsilon > 0$, $\Pr(\max_{i \in \{1,2\}} |v_i| \geq 3^{T-1}) \leq \varepsilon$ and M is the largest integer such that $3^{2M} \leq P/2$. We now construct a multi-level code with a rate of $M - T$ information bits and error probability at-most ε .

Let the information bits be represented by the vector $\mathbf{b} = (b_T, \dots, b_{M-1})$. For each $i \in \{T, \dots, M-1\}$, we map the bit $b_i \in \{0, 1\}$ into symbols $(\tilde{x}_1(i), \tilde{x}_2(i))$ according to the code construction in (41). The transmitted symbols are given by

$$x_k = \sum_{l=T}^{M-1} \tilde{x}_k(l) 3^l, \quad k = 1, 2 \quad (42)$$

and the received symbols at the two receivers can be expressed as,

$$y_1 = \sum_{l=T}^{M-1} \tilde{y}_1(l) 3^l + v_1, \quad y_2 = \sum_{l=T}^{M-1} \tilde{y}_2(l) 3^l + v_2 \quad (43)$$

where we have introduced $\tilde{y}_1(l) = \tilde{x}_1(l) + \tilde{x}_2(l)$ and $\tilde{y}_2(l) = \tilde{x}_1(l) - \tilde{x}_2(l)$.

With the choice of M , it follows that $E[|\mathbf{x}|^2] \leq P$. Furthermore in the analysis of decoding, we declare an error if $\max_i |v_i| > 3^{T-1}$. Conditioned on the fact that the $|v_i| < 3^{T-1}$ for $i = 1, 2$ note that

$$y_i - y_i \bmod 3^{T-1} \quad (44)$$

$$= y_i - \left(\sum_{l=T}^{M-1} \tilde{y}_i(l) 3^l \right) \bmod 3^T - v_i \bmod 3^T \quad (45)$$

$$= y_i - v_i = \sum_{l=T}^{M-1} \tilde{y}_i(l) 3^l. \quad (46)$$

where we have used the fact that $\left(\sum_{l=T}^{M-1} \tilde{y}_i(l) 3^l \right) \bmod 3^T = 0$ since each term in the summation is an integer multiple of 3^T .

Thus conditioned on the fact that $|v_i| < 3^{T-1}$ it is possible to retrieve $\sum_{l=T}^{M-1} \tilde{y}_i(l) 3^l$ by computing (44). Since there is no carry over across levels we in turn retrieve $(\tilde{y}_i(T), \dots, \tilde{y}_i(M))$ at each receiver. Then applying the same decoding scheme as in Prop. 5 at each level, each receiver can recover the underlying bits (b_T, \dots, b_M) . If however we have that $|v_i| \geq 3^{T-1}$, then the above analysis leading to (46) fails and an error is declared. Since T is selected to be sufficiently large, this event happens with a probability that is less than ε .

In order to complete the analysis it remains to show that $H(\mathbf{b}|z_i) = M - T$. We first enhance each eavesdropper by removing the noise variable in (40)

i.e., $\tilde{z}_j = x_j$ for $j = 1, 2$. Now consider

$$\begin{aligned} & H(b_T, \dots, b_M | \tilde{z}_i) \\ &= H(b_T, \dots, b_M | \tilde{x}_i(T), \dots, \tilde{x}_i(M)) \\ &= \sum_{l=T}^M H(b_l | \tilde{x}_i(l)) = M - T, \end{aligned}$$

where the last relation follows from $H(b_l | \tilde{x}_i(l)) = 1$ since we use the code construction in (41) in mapping $b_l \rightarrow (\tilde{x}_1(l), \tilde{x}_2(l))$.

The resulting d.o.f. achieved by the multi-level code is given by

$$d = \frac{R}{\frac{1}{2} \log P} \quad (47)$$

$$= \frac{M - T}{1/2 (2M \log_2 3 + 1)} \quad (48)$$

$$= \log_3 2 + o_M(1), \quad (49)$$

where $o_M(1) \rightarrow 0$ as $M \rightarrow \infty$. We summarize the performance of the multi-level coding scheme below.

Proposition 6: For the MISO wiretap channel with $\mathbf{h}_1 = [1, 1]$, $\mathbf{h}_2 = [1, -1]$, $\mathbf{g}_1 = [1, 0]$ and $\mathbf{g}_2 = [0, 1]$, the multi-level coding scheme can attain up-to $\frac{\log 2}{\log 3} \approx 0.63$ d.o.f.

Remark 3: We note that the achievable d.o.f. in Prop. 6 are significantly higher than those achieved by the time-sharing lower bound in Prop. 3. We show in the next section that an upper bound on secure d.o.f. in this example is $2/3$.

V. UPPER BOUND: $\min(J_r, J_e) \geq M$

In what follows we develop an upper bound on the rate of a compound wiretap code of length n . In this section we establish the following upper bound on the secure d.o.f.

Theorem 1: Consider a compound MISO wiretap channel, provided that the channel states satisfy $\min(J_r, J_e) \geq M$, the secure degrees of freedom are upper bounded by

$$d \leq 1 - \frac{1}{M^2 - M + 1} \quad (50)$$

We make a few remarks. Note that an immediate upper bound on the compound wiretap channel is the pairwise upper bound. This says that the capacity is upper bounded by

$$C \leq \max_{p_x} \min_{i,j} I(\mathbf{x}; y_i | z_j) \quad (51)$$

Intuitively this bound amounts to considering the upper bound between each receiver-eavesdropper pair and minimizing among all such pairs. To the best of our knowledge this upper bound is the only bound known for the compound wiretap channel and has been shown to be tight in some special cases [2], [14], [15]. However for the MISO wiretap channel it can be easily

verified that this upper bound results in 1 secure d.o.f. Note that with $\mathbf{x} \sim \mathcal{N}(0, \frac{P}{M}I)$

$$I(\mathbf{x}; y_i | z_j) = I(\mathbf{x}; y_i, z_j) - I(\mathbf{x}; z_j) \quad (52)$$

$$= \frac{1}{2} \log \det \left(I + \frac{P}{2} \begin{pmatrix} \mathbf{h}_i \\ \mathbf{g}_j \end{pmatrix} (\mathbf{h}_i \quad \mathbf{g}_j)^T \right) \quad (53)$$

$$- \frac{1}{2} \log \left(1 + \frac{P}{2} \|\mathbf{g}_j\|^2 \right) \quad (54)$$

which yields 1 d.o.f.

A natural improvement of the pairwise upper bound in (51) is to incorporate the fact that each receiver wants a common message i.e.,

$$C \leq \max_{p_x} \min_{i,j} \min \{ I(\mathbf{x}; y_i | z_j), I(\mathbf{x}; y_i) \} \quad (55)$$

however it can easily be verified that this potentially tighter bound also yields 1 d.o.f. To get a tighter bound in Thm. 1 we start from first principles and carefully combine the constraints imposed by the secrecy requirements and the common message transmission.

The proof of the upper bound will be presented in the full paper.

ACKNOWLEDGEMENTS

Insightful discussions with Frank Kschischang and Suhas Diggavi are gratefully acknowledged.

REFERENCES

- [1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.
- [2] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting over fading channels," *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 2008.
- [3] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, Oct., 2008.
- [4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, June, 2008.
- [5] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. Int. Symp. Inform. Theory*, Nice, 2007.
- [6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *To Appear, IEEE Trans. Inform. Theory*.
- [7] —, "Secure transmission with multiple antennas: The MIMOME wiretap channel," *To Appear, IEEE Trans. Inform. Theory*.
- [8] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, July, 2009, submitted.
- [9] R. Liu, T. Liu, H. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, To Appear.
- [10] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inform. Theory*, June, 2009.
- [11] 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. Inform. Theory*, Sept., 2009.
- [12] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel," *IEEE Trans. Inform. Theory*, March, 2009, submitted.
- [13] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy capacity region of gaussian broadcast channel," in *CISS*, 2009.
- [14] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wire-tap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, submitted 2008.
- [15] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of non-degraded parallel gaussian compound wiretap channels," Jul. 2008.
- [16] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inform. Theory*, Oct., 2009, submitted.
- [17] E. Perron, S. N. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *INFOCOM*, April 2009.
- [18] X. He and A. Yener, "Secure degrees of freedom for gaussian channels with interference: Structured codes outperform gaussian signaling," *IEEE Trans. Inform. Theory*.
- [19] O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inform. Theory*, Oct. 2008, submitted.
- [20] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure dof of the single-antenna mac," in *Proc. Int. Symp. Inform. Theory*, 2010, submitted.
- [21] G. Golub and C. F. V. Loan, *Matrix Computations (3rd ed)*. Johns Hopkins University Press, 1996.