On the Secrecy of Multiple Access Wiretap Channel

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

***Abstract*— We develop an outer bound for the secrecy capacity region of a class of multiple access wiretap channels (MAC-WT). In this class, which we call the *weak eavesdropper* class, each user's link to the legitimate receiver is stronger than its link to the eavesdropper. Our outer bound partially matches the achievable region in an n-letter form. In addition, a looser version of our outer bound provides close approximations to the capacity region of the Gaussian MAC-WT channel. In particular, we prove that our outer bound is within 0.5 bits/channel use of the achievable rates along the individual rates for all weak eavesdropper Gaussian MAC-WT, and within 0.5 bits/channel use in all directions for certain weak eavesdropper Gaussian MAC-WT channels.**

I. Introduction

Information theoretic secrecy has attracted a considerable amount of interest recently. Following the pioneering works of Wyner [1] and Csiszar and Korner [2] who studied the single-transmitter single-receiver single-eavesdropper wiretap channel, many multi-user channel models have been considered from a secrecy point of view.

The multiple access wiretap channel (MAC-WT) is introduced in [3], [4]. In MAC-WT, there is an eavesdropper in addition to the ordinary MAC; see Figure 1. For this channel, an achievable scheme is proposed in [3], where also the sum secrecy capacity of the degraded Gaussian channel is found. In [4], a general, not necessarily degraded, Gaussian MAC-WT is considered, and achievable sum secrecy rate maximization problems are studied.

We consider a class of MAC-WT where each user's link to the legitimate receiver is stronger than its link to the eavesdropper. We call this class of MAC-WT the *weak eavesdropper* class. We develop an n-letter outer bound for this class, which partially matches the achievable region. Even though the matching achievable region and the outer bound give us the capacity, unfortunately, the capacity expressions are in n-letter form, and are not computable. We then consider a Gaussian MAC-WT which satisfies the *weak eavesdropper* condition. We develop a looser outer bound for this Gaussian case. This looser version of our outer bound for the Gaussian MAC-WT yields close approximations to the capacity region along the individual rate axes. In particular, we show that the gap between our inner and outer bounds is independent of the channel parameters, and is less than 0.5 bits/channel use.

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

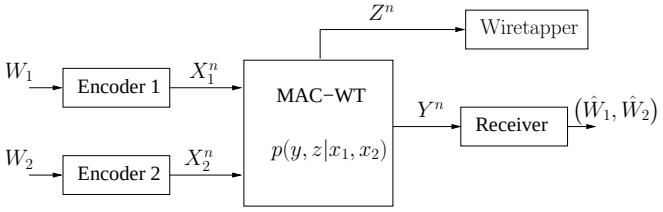

Fig. 1. The multiple access wiretap channel (MAC-WT).

We then consider a special class of weak eavesdropper Gaussian MAC-WT, where each user has an orthogonal link to the legitimate receiver, while the channel from the users to the eavesdropper is a general MAC. In this case, our outer bound yields close approximations to the capacity region not only along the individual rate dimensions, but also for the sum rate line. In particular, we show that these gaps are independent of the channel parameters, and are all less than 0.5 bits/channel use. Furthermore, for a set of specific channel parameters, we obtain the exact sum secrecy capacity.

In the final part of this paper, we discuss the implications of our results on the degraded MAC-WT which, by definition, belongs to the weak eavesdropper class studied in this paper. Moreover, we consider the interference wiretap channel (IC-WT) which consists of an ordinary interference channel (IC) and an eavesdropper listening to the ongoing communication in the IC. The similarity between the IC-WT with *very strong* interference among the users and the weak eavesdropper Gaussian MAC-WT with orthogonal components is discussed.

II. Channel Model

The MAC-WT (Figure 1) consists of two input alphabets, $\mathcal{X}_1, \mathcal{X}_2$, and two output alphabets, $\mathcal{Y}, \mathcal{Z}$. The channel is assumed to be memoryless with conditional distribution $p(y, z|x_1, x_2)$. The inputs can be selected from product distributions on $\mathcal{X}_1 \times \mathcal{X}_2$. A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two independent message sets $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}, \mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, two encoders $f_i : \mathcal{W}_i \rightarrow \mathcal{X}_i^n$, $i = 1, 2$, and a decoder $g : \mathcal{Y}^n \rightarrow \mathcal{W}_1 \times \mathcal{W}_2$. The error probability is $P_e^n = \Pr\left(g(Y^n) \neq (W_1, W_2)\right)$. The secrecy of the users is measured by the equivocation rates at the eavesdropper which are $\frac{1}{n}H(W_1|Z^n)$, $\frac{1}{n}H(W_2|Z^n)$ and $\frac{1}{n}H(W_1, W_2|Z^n)$. A rate pair, (R_1, R_2), is said to be achiev-

able with perfect secrecy if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code satisfying $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Z^n) \geq R_1 \tag{1}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_2|Z^n) \geq R_2 \tag{2}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_1, W_2|Z^n) \geq R_1 + R_2 \tag{3}$$

Thus, we only consider *perfect* secrecy in this paper.

The Gaussian MAC-WT is given by

$$Y = X_1 + X_2 + N_y \tag{4}$$

$$Z = \sqrt{h_1} X_1 + \sqrt{h_2} X_2 + N_z \tag{5}$$

where N_y and N_z are i.i.d. Gaussian random variables with zero-mean and unit-variance. We have average power constraints on the channel inputs: $E\left[X_j^2\right] \leq P_j,\ j = 1, 2$.

III. MAC-WT with Weak Eavesdropper

We define the weak eavesdropper MAC-WT channels as those that satisfy

$$I(X_1; Y|X_2) \geq I(X_1; Z|X_2) \tag{6}$$

$$I(X_2; Y|X_1) \geq I(X_2; Z|X_1) \tag{7}$$

for all joint input distributions of the form $p(x_1, x_2) = p(x_1)p(x_2)$. This condition can be interpreted as requiring each user to have a *more capable* channel to its legitimate receiver in the absence of the other user.

We first state an achievable region for the *general* MAC-WT in the following theorem.

Theorem 1: The rate pairs (R_1, R_2) satisfying

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n)\right]^+ \tag{8}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y^n|X_1^n) - I(X_2^n; Z^n)\right]^+ \tag{9}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n)\right]^+ \tag{10}$$

are achievable with perfect secrecy for any distribution of the form $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

In Theorem 1, $(\cdot)^+$ denotes the positivity operator, i.e., $(x)^+ = \max(0, x)$. This theorem is an extension of the achievable region provided in [3], hence its proof is omitted.

For a MAC-WT channel satisfying (6)-(7), the rates in (8)-(9) are always positive [5]. Thus, as long as we consider channels that satisfy (6)-(7), we do not need the positivity operators in (8)-(9). However, we note that the conditions in (6)-(7) do not imply the positivity of the achievable sum secrecy rate in (10). Therefore, even in the weak eavesdropper MAC-WT, we do need the positivity operator in (10). The following corollary states these observations formally.

Corollary 1: For weak eavesdropper MAC-WT, the rate pairs (R_1, R_2) satisfying

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n)\right] \tag{11}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y^n|X_1^n) - I(X_2^n; Z^n)\right] \tag{12}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n)\right]^+ \tag{13}$$

are achievable with perfect secrecy for any distribution of the form $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

Next, we provide our outer bound on the secrecy capacity of the weak eavesdropper MAC-WT.

Theorem 2: The secrecy capacity region of a weak eavesdropper MAC-WT lies in the union of the rates satisfying

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n)\right] \tag{14}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y^n|X_1^n) - I(X_2^n; Z^n)\right] \tag{15}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \big[I(X_1^n; Y^n|X_2^n) + I(X_2^n; Y^n|X_1^n) - I(X_1^n, X_2^n; Z^n)\big] \tag{16}$$

where the union is taken over all $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

This theorem is proved in Appendix I. The difference between our inner and outer bounds for the weak eavesdropper MAC-WT is in the sum secrecy rate expressions in (13) and (16). Apart from these, the individual achievable secrecy rate terms in (11)-(12) and the individual secrecy rate upper bounds in (14)-(15) match, yielding a partial characterization of the secrecy capacity region in an n-letter form.

IV. Gaussian MAC-WT with Weak Eavesdropper

Gaussian MAC-WT channels that satisfy the weak eavesdropper conditions in (6)-(7) have $h_1, h_2 < 1$; see Appendix II for a proof. For the weak eavesdropper Gaussian MAC-WT (as for any weak eavesdropper MAC-WT), the identical inequalities in (11)-(12) and (14)-(15) give the secrecy capacity along the individual rate axes. However, the difficulty is, even for Gaussian channels, finding the optimal input distributions $p(x_1^n)$, $p(x_2^n)$ and evaluating the boundary of (11)-(12) and (14)-(15) seems to be intractable for now. Consequently, we loosen our outer bound to obtain computable expressions. We show however that even the loosened outer bound is within 0.5 bits/channel use of the achievable region along the individual rate dimensions. We give our loosened outer bound in the following theorem, which we prove in Appendix II.

Theorem 3: The secrecy capacity region of Gaussian MAC-WT with $h_1, h_2 < 1$ is contained in the following region.

$$R_1 \leq \frac{1}{2}\log\left(1 + P_1\right) - \frac{1}{2}\log\left(\frac{2 + h_1P_1 + h_2P_2}{2(1 + h_2P_2)}\right) \tag{17}$$

$$R_2 \leq \frac{1}{2}\log\left(1 + P_2\right) - \frac{1}{2}\log\left(\frac{2 + h_1P_1 + h_2P_2}{2(1 + h_1P_1)}\right) \tag{18}$$

Next, we compare our outer bound in Theorem 3 with our achievable rates in Corollary 1. The optimum set of achievable rates that Corollary 1 gives is not known. However, we can always obtain potentially sub-optimal achievable rates by using i.i.d. (in time) Gaussian signalling. We note that the

ultimate achievable rates thus calculated may yield either a pentagon, a triangle or a trapezoid, as the sum rate expression in (13) may dominate the individual rates in (11) and (12). Since our aim is to investigate how far our outer bound is from the achievable region along the individual rate axes, we will choose our parameters to guarantee that we do not have a triangle as an achievable region. Thus, let us assume that h_1, h_2, P_1, P_2 are such that at least one of the inequalities

$$h_1 \leq \frac{1}{1+P_2}, \quad h_2 \leq \frac{1}{1+P_1} \tag{19}$$

is satisfied so that we have either a trapezoid or a pentagon as an achievable region; see Figure 2. Then, we have the following achievable rates expressed in four different possible cases.

Corollary 2: Without loss of generality, we assume $h_1 < h_2 < 1$. The following secrecy regions are achievable.

- Case I: $h_1 \leq \frac{1}{1+P_2}$, $h_2 \leq \frac{1}{1+P_1}$

$$R_1 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \tag{20}$$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{21}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{22}$$

- Case II: $h_1 \leq \frac{1}{1+P_2}$, $\frac{1}{1+P_1} \leq h_2 \leq \frac{1+h_1P_1}{1+P_1}$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{23}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{24}$$

- Case III: $h_1 \leq \frac{1}{1+P_2}$, $\frac{1+h_1P_1}{1+P_1} \leq h_2$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{25}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log(1+h_1P_1) \tag{26}$$

- Case IV: $\frac{1}{1+P_2} \leq h_1$, $h_2 \leq \frac{1}{1+P_1}$

$$R_1 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \tag{27}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{28}$$

The achievable regions in Corollary 2 are obtained by using i.i.d. (in time) Gaussian signalling in Corollary 1. We now check the gap between our inner and outer bounds on the individual rates. Here, as an example, we evaluate the difference between the achievable rate and the outer bound for user 1, i.e., the difference of (20) and (27) with (17); such difference for the rate of user 2 can be calculated similarly. For user 1, this difference is:

$$\frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right) = \frac{1}{2}\log\left(\frac{2(1+h_1P_1+h_2P_2)}{2+h_1P_1+h_2P_2}\right) \tag{29}$$

which is always less than 0.5 bits/channel use. Thus, if the first (resp. second) inequality in (19) is satisfied, then the secrecy rate achievable for the second (resp. first) user via i.i.d. Gaussian signalling and without pre-processing is within half bit of the maximum possible secrecy rate for that user. A graphical illustration of our inner and outer bounds is given in Figure 2.

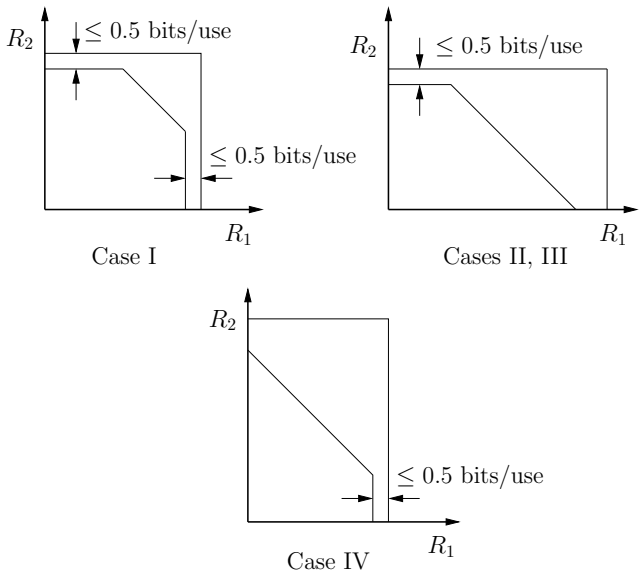

Fig. 2. Illustration of outer and inner bounds for different h_1, h_2 values.

V. A Special Class: Orthogonal Components

We now consider a special sub-class of weak eavesdropper Gaussian MAC-WT class where each user has an orthogonal link to the legitimate receiver while the links from the users to the eavesdropper form a general Gaussian MAC:

$$Y_1 = X_1 + N_{y1} \tag{30}$$

$$Y_2 = X_2 + N_{y2} \tag{31}$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_z \tag{32}$$

where N_{y1}, N_{y2} and N_z are i.i.d. zero-mean unit-variance Gaussian random variables. Here again we have $h_1, h_2 < 1$. We have the following achievable region.

Corollary 3: The following region is achievable for the orthogonal-component weak eavesdropper Gaussian MAC-WT

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \quad (33)$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \quad (34)$$

$$R_1+R_2 \leq \frac{1}{2}\log\left(1+P_1\right) + \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(1+h_1P_1+h_2P_2\right) \quad (35)$$

This achievable region is obtained by using i.i.d. (in time) Gaussian signalling in Corollary 1. We have the following outer bound on the secrecy capacity region of this channel.

Theorem 4: The secrecy capacity region of the orthogonal-component weak eavesdropper Gaussian MAC-WT is contained in the following region.

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right) \quad (36)$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_1P_1)}\right) \quad (37)$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1) + \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2}\right) \quad (38)$$

This theorem is proved in Appendix III. Thus, for this special class of channels, using a calculation similar to that in (29), we can show that the difference between the sum secrecy rate expressions on the right hand sides of (35) and (38) is less than 0.5 bits/channel use. The situation in this special weak eavesdropper Gaussian MAC-WT is illustrated in Figure 3.

Moreover, if we restrict the channel gains to $h_1+h_2<1$, then we can determine the sum secrecy capacity of this channel as stated in the next theorem, which we prove in Appendix IV.

Theorem 5: If $h_1+h_2<1$, then the sum secrecy capacity of this channel is given by

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1) + \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \quad (39)$$

VI. Further Remarks

We now discuss the implications of our results on the secrecy capacity of the degraded MAC-WT. Degraded MAC-WT satisfies the Markov chain

$$(X_1,X_2) \to Y \to Z \quad (40)$$

and consequently, satisfies the conditions given in (6)-(7). Thus, our outer bound in Theorem 2 holds for these channels as well. Indeed, our Theorem 2 can be improved to give the entire capacity region in an n-letter form as given in the following theorem.

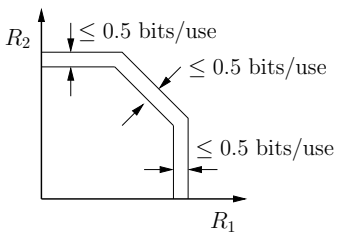

Fig. 3. Illustration of outer and inner bounds for MAC-WT with orthogonal components.

Theorem 6: The secrecy capacity region of a degraded MAC-WT is given by the union of the following rates

$$R_1 \leq \lim_{n\to\infty}\frac{1}{n}\left[I(X_1^n;Y^n|X_2^n) - I(X_1^n;Z^n)\right] \quad (41)$$

$$R_2 \leq \lim_{n\to\infty}\frac{1}{n}\left[I(X_2^n;Y^n|X_1^n) - I(X_2^n;Z^n)\right] \quad (42)$$

$$R_1+R_2 \leq \lim_{n\to\infty}\frac{1}{n}\left[I(X_1^n,X_2^n;Y^n) - I(X_1^n,X_2^n;Z^n)\right] \quad (43)$$

where the union is taken over all $p(x_1^n,x_2^n)=p(x_1^n)p(x_2^n)$.

The proof of Theorem 6 is given in Appendix V. We further remark that the sum secrecy capacity of the degraded MAC-WT can be put into a single-letter form as $I(X_1,X_2;Y|Z)$.

As a result of Theorem 6, we establish the secrecy capacity region of the degraded MAC-WT in n-letter form. Prior to our result here, only the sum secrecy capacity of the degraded Gaussian MAC-WT was known due to [3], where the degraded Gaussian MAC-WT is defined by (4)-(5) with $h_1=h_2=h<1$. Hence, using our outer bound in Theorem 3, and with the sum rate capacity result of [3], we have the following corollary for the degraded Gaussian MAC-WT.

Corollary 4: The achievable region described by (20)-(22) coincides with the sum secrecy rate points of the degraded Gaussian MAC-WT. Moreover, this region is within half bit of the straight lines of the pentagon corresponding to the capacity region if $h \leq \min\left(1/(1+P_1), 1/(1+P_2)\right)$.

In Corollary 4, the claim regarding the sum secrecy capacity is due to [3]. The other claim can be proved by simply setting $h_1=h_2=h$ in Theorem 3 and in Corollary 2, and checking the gap between these rates as it is done in (29).

A further remark is about IC-WT when the interference among the users is *very strong*. We now show that the results obtained for the Gaussian MAC-WT with orthogonal components in Section V hold for IC-WT with very strong interference as well. The Gaussian IC-WT is defined by

$$Y_1 = X_1 + \sqrt{\alpha}X_2 + N_{y1} \quad (44)$$

$$Y_2 = X_2 + \sqrt{\beta}X_1 + N_{y2} \quad (45)$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_z \quad (46)$$

where Y_1, Y_2 and Z denote the users' and the eavesdropper's observation, respectively. We have power constraints on the

channel inputs as $E\left[X_j^2\right] \leq P_j,\ j=1,2$ and the channel inputs should be independent. All of the definitions in Section II regarding the codes and the achievability hold for IC-WT with appropriate modifications. Since there are now two receivers, we have two decoders, each one associated with one receiver. Consequently, each decoder has its own probability of error that needs to decay to zero. Similar to MAC-WT, each transmitter uses a codebook that is independent of the other user's codebook and the secrecy is measured through $\frac{1}{n}H(W_1|Z^n), \frac{1}{n}H(W_2|Z^n), \frac{1}{n}H(W_1,W_2|Z^n)$.

If α and β satisfy

$$\alpha \geq 1+P_1, \quad \beta \geq 1+P_2 \tag{47}$$

interference at each terminal becomes *very strong* which can be eliminated entirely leaving each user a clean, single-user channel [6]. Consequently, the resulting channel becomes equivalent to the channel in (30)-(32). Thus, in light of the results obtained in Section V, we find the secrecy capacity region of this channel to within half bit. This is stated in the next theorem which is proved in Appendix VI.

Theorem 7: The achievable secrecy region given in Corollary 3 is within half bit of the secrecy capacity region of the IC-WT if α and β satisfy (47) and $h_1, h_2 < 1$. Moreover, if $h_1+h_2<1$, then the sum secrecy capacity is given by (39).

VII. Conclusions

We focused on a special class of MAC-WT which we call the *weak eavesdropper* MAC-WT. We developed an n-letter outer bound for the perfect secrecy capacity of this class of channels. This n-letter outer bound matches the achievable region partially. Although this partial matching gives us a limited characterization of the capacity region, it is in an n-letter form, and is incomputable. Focusing our attention to Gaussian channels, we were able to evaluate a looser version of our bound which determines the secrecy capacity region along individual rates axes within half bit irrespective of the channel parameters. We then considered a special class of *weak eavesdropper* MAC-WT where each user has an orthogonal link to the legitimate receiver. For this class of channels, a looser version of our outer bound determines the entire capacity region within half bit. Furthermore, implications of our results on the degraded MAC-WT as well as on the IC-WT with strong interference are addressed.

Appendix I
Proof of Theorem 2

First, we note that for channels satisfying (6)-(7), we also have

$$I(X_1^n;Y^n|X_2^n,U) \geq I(X_1^n;Z^n|X_2^n,U) \tag{48}$$
$$I(X_2^n;Y^n|X_1^n,U) \geq I(X_2^n;Z^n|X_1^n,U) \tag{49}$$

for all $p(x_1^n,x_2^n)=p(x_1^n)p(x_2^n)$ and any random variable U such that $U \rightarrow (X_1^n,X_2^n) \rightarrow (Y^n,Z^n)$, $X_1^n \rightarrow U \rightarrow X_2^n$ [5]. Thus, using this result, we can obtain

$$I(X_1^n;Y^n|X_2^n,W_1) \geq I(X_1^n;Z^n|X_2^n,W_1) \tag{50}$$
$$\geq I(X_1^n;Z^n|W_1) \tag{51}$$

where in the second inequality, we use the fact that (X_1^n,W_1) and X_2^n are independent, and that conditioning decreases entropy. Similarly, we have

$$I(X_2^n;Y^n|X_1^n,W_2) \geq I(X_2^n;Z^n|X_1^n,W_2) \tag{52}$$
$$\geq I(X_2^n;Z^n|W_2) \tag{53}$$

Furthermore, starting with (48), we get

$$I(X_1^n;Y^n|X_2^n,W_1) \geq I(X_1^n;Z^n|X_2^n,W_1) \tag{54}$$
$$= I(X_1^n;Z^n|X_2^n,W_1,W_2) \tag{55}$$
$$\geq I(X_1^n;Z^n|W_1,W_2) \tag{56}$$

where the equality is due to the fact that given X_2^n, W_2 is independent of everything else and the last inequality follows from the fact that (X_1^n,W_1) and (X_2^n,W_2) are independent and that conditioning decreases entropy. If we combine (56) with

$$I(X_2^n;Y^n|X_1^n,W_2) \geq I(X_2^n;Z^n|X_1^n,W_2,W_1) \tag{57}$$

which follows from (55) due to symmetry, we get

$$I(X_1^n;Y^n|X_2^n,W_1)+I(X_2^n;Y^n|X_1^n,W_2) \geq I(X_1^n,X_2^n;Z^n|W_1,W_2) \tag{58}$$

which will be used in the derivation of our outer bound on the sum secrecy rate. Hence, we have all the necessary inequalities, i.e., (51), (53), (58), for the remaining part of the proof.

We start with the derivation of our outer bound on R_1,

$$nR_1 \leq H(W_1|Z^n) \leq I(W_1;Y^n)-I(W_1;Z^n)+\epsilon_n \tag{59}$$
$$\leq I(W_1;Y^n|X_2^n)-I(W_1;Z^n)+\epsilon_n \tag{60}$$
$$\leq I(W_1;Y^n|X_2^n)-I(W_1;Z^n)+\epsilon_n + I(X_1^n;Y^n|X_2^n,W_1)-I(X_1;Z^n|W_1) \tag{61}$$
$$= I(W_1,X_1^n;Y^n|X_2^n)-I(W_1,X_1^n;Z^n)+\epsilon_n \tag{62}$$
$$= I(X_1^n;Y^n|X_2^n)-I(X_1^n;Z^n)+\epsilon_n \tag{63}$$

where (59) is due to Fano's lemma [7], (60) is due to the fact that W_1 and X_2^n are independent and that conditioning decreases entropy, (61) is obtained by using (51), and (63) follows from the fact that given X_1^n, W_1 is independent of everything else. This gives us (14). Similarly, one can get (15).

We next prove our outer bound on the sum secrecy rate.

$$n(R_1+R_2) \leq H(W_1,W_2|Z^n) \tag{64}$$
$$\leq I(W_1,W_2;Y^n)-I(W_1,W_2;Z^n)+\epsilon_n \tag{65}$$
$$\leq I(W_1;Y^n|X_2^n)+I(W_2;Y^n|X_1^n)-I(W_1,W_2;Z^n)+\epsilon_n \tag{66}$$
$$\leq I(W_1;Y^n|X_2^n)+I(W_2;Y^n|X_1^n)-I(W_1,W_2;Z^n) + I(X_1^n;Y^n|X_2^n,W_1)+I(X_2^n;Y^n|X_1^n,W_2) - I(X_1^n,X_2^n;Z^n|W_1,W_2)+\epsilon_n \tag{67}$$
$$= I(X_1^n;Y^n|X_2^n)+I(X_2^n;Y^n|X_1^n) - I(X_1^n,X_2^n;Z^n)+\epsilon_n \tag{68}$$

where (65) is due to Fano's lemma [7], (66) follows from the

fact that W_1 (resp. W_2) and X_2^n (resp. X_1^n) are independent and that conditioning decreases entropy, (67) follows by using (58) and (68) comes from the fact that given X_1^n (resp. X_2^n)), W_1 (resp. W_2) is independent of everything else. This gives us (16).

Appendix II
Proof of Theorem 3

First, we show that Gaussian MAC-WT with $h_1, h_2 < 1$ satisfies (6)-(7), hence Theorem 2 is applicable. To this end, define the following random variables

$$\tilde{Y}_1 = Y - X_2 = X_1 + N_y \tag{69}$$

$$\tilde{Z}_1 = \sqrt{h_1}(X_1 + N_y) + \sqrt{1-h_1}\tilde{N} \tag{70}$$

where $\tilde{N} \sim \mathcal{N}(0,1)$ and is independent of everything else. Note that $\tilde{Y}_1$ and $\tilde{Z}_1$ satisfy

$$I(X_1; Y|X_2) = I(X_1; \tilde{Y}_1) = I(X_1; \tilde{Y}_1, \tilde{Z}_1) \tag{71}$$

$$I(X_1; Z|X_2) = I(X_1; \tilde{Z}_1) \tag{72}$$

where the second equality of (71) is due to the Markov chain $X_1 \to \tilde{Y}_1 \to \tilde{Z}_1$. Thus, we have

$$I(X_1; Y|X_2) - I(X_1; Z|X_2) = I(X_1; \tilde{Y}_1, \tilde{Z}_1) - I(X_1; \tilde{Z}_1) \tag{73}$$

$$= I(X_1; \tilde{Y}_1|\tilde{Z}_1) \geq 0 \tag{74}$$

proving that Gaussian MAC-WT with $h_1, h_2 < 1$ satisfies (6)-(7).

We now bound the following term

$$\begin{aligned} &I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n) \\ &= H(X_1^n + N_y^n) + H(\sqrt{h_2}X_2^n + N_z^n) \\ &\quad - H(\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + N_z^n) - H(N_y^n) \end{aligned} \tag{75}$$

where we use $H(\cdot)$ to denote the differential entropy of a continuous random variable. We will use a variant of the entropy-power inequality given in [8]. Let $\{U_i^n\}_{i=1}^N$ be independent length-n random vectors. If $\mathcal{C}$ denotes an arbitrary collection of subsets of $\{1, \ldots, N\}$, then we have

$$\exp\left(\frac{2}{n}H\left(\sum_{i=1}^N U_i^n\right)\right) \geq \frac{1}{r}\sum_{\mathbf{S}\in\mathcal{C}} \exp\left(\frac{2}{n}H\Big(\sum_{i\in\mathbf{S}} U_i^n\Big)\right) \tag{76}$$

where r denotes the maximum number of subsets in $\mathcal{C}$ in which any one index, i, appears, and $\mathbf{S}$ denotes a subset of $\{1, \ldots, n\}$ that is in the collection $\mathcal{C}$.

Before using this inequality, first decompose N_z^n as follows

$$N_z^n = \sqrt{h_1}N_y^n + \sqrt{1-h_1}\tilde{N}^n \tag{77}$$

where $\tilde{N}^n \sim \mathcal{N}(0, \mathbf{I})$ and is independent of everything else. Furthermore, let us define

$$t_1 = H(X_1^n + N_y^n) \tag{78}$$

$$= H(\sqrt{h_1}X_1^n + \sqrt{h_1}N_y^n) - \frac{n}{2}\log(h_1) \tag{79}$$

and

$$t_2 = H(\sqrt{h_2}X_2 + N_z^n) \tag{80}$$

$$= H(\sqrt{h_2}X_2^n + \sqrt{h_1}N_y^n + \sqrt{1-h_1}\tilde{N}^n) \tag{81}$$

Using the inequality in (76), we have the following lower bound

$$\begin{aligned} &H(\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + N_z^n) \geq \\ &\frac{n}{2}\log\left(\frac{h_1}{2}\exp\left(\frac{2t_1}{n}\right) + \frac{1}{2}\exp\left(\frac{2t_2}{n}\right) + 2\pi e\frac{1-h_1}{2}\right) \end{aligned} \tag{82}$$

Using (75) and (82), we obtain the following upper bound

$$I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n) \leq \max_{t_1,t_2} f(t_1, t_2) \tag{83}$$

where $f(t_1, t_2)$ is

$$\begin{aligned} &f(t_1, t_2) = t_1 + t_2 \\ &- \frac{n}{2}\log\left(\frac{h_1}{2}\exp\left(\frac{2t_1}{n}\right) + \frac{1}{2}\exp\left(\frac{2t_2}{n}\right) + 2\pi e\frac{1-h_1}{2}\right) \\ &- \frac{n}{2}\log(2\pi e) \end{aligned} \tag{84}$$

Note that $f(t_1, t_2)$ is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when $X_1^n \sim \mathcal{N}(0, P_1\mathbf{I})$ and $X_2^n \sim \mathcal{N}(0, P_2\mathbf{I})$, the maximum value of $f(t_1, t_2)$ is

$$\frac{1}{2}\log(1+P_1) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right) \tag{85}$$

This completes the proof of the upper bound on R_1 given in (17). The upper bound on R_2 given in (18) follows from symmetry.

Appendix III
Proof of Theorem 4

We define $Y^n = (Y_1^n, Y_2^n)$. Using the facts that X_1^n (resp. X_2^n) and Y_2^n (resp. X_1^n) are independent, we get

$$I(X_1^n; Y^n|X_2^n) = I(X_1^n; Y_1^n) \tag{86}$$

$$I(X_2^n; Y^n|X_1^n) = I(X_2^n; Y_2^n) \tag{87}$$

$$I(X_1^n, X_2^n; Y^n) = I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) \tag{88}$$

Moreover, following the analysis carried out in the proof of Theorem 3 in Appendix II, we can show that this channel satisfies (6)-(7). Thus, our outer bound in Theorem 2 can be applied to this channel as well. Hence, plugging the expressions in (86)-(88) into Corollary 1 and Theorem 2, we get the secrecy capacity region of this channel as follows.

$$R_1 \leq \lim_{n\to\infty}\frac{1}{n}\left[I(X_1^n; Y_1^n) - I(X_1^n; Z^n)\right] \tag{89}$$

$$R_2 \leq \lim_{n\to\infty}\frac{1}{n}\left[I(X_2^n; Y_2^n) - I(X_2^n; Z^n)\right] \tag{90}$$

$$\begin{aligned} R_1 + R_2 \leq \lim_{n\to\infty}\frac{1}{n}\big[&I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) \\ &- I(X_1^n, X_2^n; Z^n)\big] \end{aligned} \tag{91}$$

As opposed to the general weak eavesdropper MAC-WT class, for this sub-class, we are able to obtain the entire

secrecy capacity region in an n-letter form, because the expression in (13) is guaranteed to be positive, and the expressions in (13) and (16) become identical, due to (86)-(88). The two bounds on the individual secrecy rate terms are identical to those in the proof of Theorem 3 given in Appendix II, and hence the bounds in Theorem 3 directly apply for this channel as well. Hence, we only need to consider the sum secrecy rate term which is

$$\begin{aligned} &I(X_1^n;Y_1^n)+I(X_2^n;Y_2^n)-I(X_1^n,X_2^n;Z^n) \\ &= H(X_1^n+N_{y1}^n)+H(X_2^n+N_{y2}^n) \\ &\quad - H(\sqrt{h_1}X_1^n+\sqrt{h_2}X_2^n+N_z^n)-\frac{n}{2}\log(2\pi e) \end{aligned} \tag{92}$$

We decompose the noise of the eavesdropper as

$$N_z^n=\sqrt{h_1}\tilde{N}_1^n+\sqrt{h_2-h_1}\tilde{N}_2^n+\sqrt{1-h_2}\tilde{N}_3^n \tag{93}$$

where $\tilde{N}_1^n,\tilde{N}_2^n,\tilde{N}_3^n$ are independent Gaussian random vectors with zero-mean and identity covariance matrices. We also define

$$t_1 = H(X_1^n+N_{y1}^n) \tag{94}$$

$$= H(\sqrt{h_1}X_1^n+\sqrt{h_1}\tilde{N}_1^n)-\frac{n}{2}\log h_1 \tag{95}$$

and

$$t_2 = H(X_2^n+N_{y2}^n) \tag{96}$$

$$= H(\sqrt{h_2}X_2^n+\sqrt{h_2-h_1}\tilde{N}_2^n+\sqrt{h_1}\tilde{N}_1^n)-\frac{n}{2}\log h_2 \tag{97}$$

Using the entropy power inequality of [8] given in (76), we get

$$\frac{2}{n}H(\sqrt{h_1}X_1^n+\sqrt{h_2}X_2^n+N_z^n)\geq g(t_1,t_2) \tag{98}$$

where $g(t_1,t_2)$ is

$$\log\left(\frac{h_1}{2}\exp\left(\frac{2t_1}{n}\right)+\frac{h_2}{2}\exp\left(\frac{2t_2}{n}\right)+2\pi e\frac{2-h_2-h_1}{2}\right) \tag{99}$$

Thus, the sum secrecy rate can be upper bounded as

$$I(X_1^n;Y_1^n)+I(X_2^n;Y_2^n)-I(X_1^n,X_2^n;Z^n)\leq\max_{t_1,t_2}f(t_1,t_2) \tag{100}$$

where $f(t_1,t_2)$ is

$$\frac{2}{n}f(t_1,t_2)=\frac{2}{n}(t_1+t_2)+\log(2\pi e)-g(t_1,t_2) \tag{101}$$

which is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when $X_1^n\sim\mathcal{N}(0,P_1\mathbf{I})$ and $X_2^n\sim\mathcal{N}(0,P_2\mathbf{I})$, the maximum value of $f(t_1,t_2)$ is

$$\begin{aligned} &\frac{1}{2}\log(1+P_1)+\frac{1}{2}\log(1+P_2) \\ &\qquad -\frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2}\right) \end{aligned} \tag{102}$$

This completes the proof of the upper bound on the sum secrecy rate given in (38).

Appendix IV
Proof of Theorem 5

The proof of Theorem 5 is similar to the proof of the sum rate secrecy bound in Theorem 4. The differences are in the way we decompose the eavesdropper noise and apply the entropy power inequality. Here, the classical entropy power inequality [9], [10] is sufficient to get the result, i.e, we do not make use of the additional properties of the one in (76) [8]. Instead of decomposing the noise as in (93), we will use

$$N_z^n=\sqrt{h_1}N_{y1}^n+\sqrt{h_2}N_{y2}^n+\tilde{N}^n \tag{103}$$

where $\tilde{N}^n$ is i.i.d. Gaussian noise sequence with zero-mean and variance of $1-h_1-h_2$. Consequently, using entropy power inequality, we get

$$\frac{2}{n}I(X_1^n,X_2^n;Z^n)$$

$$= \frac{2}{n}H(\sqrt{h_1}X_1^n+\sqrt{h_2}X_2^n+N_z^n)-\log(2\pi e) \tag{104}$$

$$\geq g(t_1,t_2) \tag{105}$$

where $g(t_1,t_2)$ is

$$\log\left(\frac{h_1}{2\pi e}\exp\left(\frac{2t_1}{n}\right)+\frac{h_2}{2\pi e}\exp\left(\frac{2t_2}{n}\right)+1-h_1-h_2\right) \tag{106}$$

and t_1,t_2 are

$$t_1 = H\left(X_1^n+N_{y1}^n\right) \tag{107}$$

$$t_2 = H\left(X_2^n+N_{y2}^n\right) \tag{108}$$

Therefore, the sum secrecy rate can be upper bounded as

$$I(X_1^n;Y_1^n)+I(X_2^n;Y_2^n)-I(X_1^n,X_2^n;Z^n)\leq\max_{t_1,t_2}f(t_1,t_2) \tag{109}$$

where $f(t_1,t_2)$ is

$$\frac{2}{n}f(t_1,t_2)=\frac{2}{n}(t_1+t_2)-2\log(2\pi e)-g(t_1,t_2) \tag{110}$$

which is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when X_1^n,X_2^n are selected as Gaussian with zero-mean and covariance matrices of $P_1\mathbf{I},P_2\mathbf{I}$, we get

$$\begin{aligned} &I(X_1^n;Y_1^n)+I(X_2^n;Y_2^n)-I(X_1^n,X_2^n;Z^n) \\ &\qquad\leq \frac{n}{2}\log(1+P_1)+\frac{n}{2}\log(1+P_2) \\ &\qquad\quad -\frac{n}{2}\log(1+h_1P_1+h_2P_2) \end{aligned} \tag{111}$$

which completes the proof.

Appendix V
Proof of Theorem 6

Since degraded channels already satisfy the conditions in (6)-(7), the outer bound in Theorem 2 is valid for them. Thus, to prove Theorem 6, we only need to consider the

sum secrecy rate. First, note that for degraded channels

$$I(X_1^n, X_2^n; Y^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n|W_1, W_2)$$
$$= I(X_1^n, X_2^n; Y^n, Z^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n|W_1, W_2) \quad (112)$$
$$= I(X_1^n, X_2^n; Y^n|W_1, W_2, Z^n) \quad (113)$$
$$\geq 0 \quad (114)$$

where the first equality is due to the degradedness. We now bound sum secrecy rate of the degraded channels.

$$H(W_1, W_2|Z^n)$$
$$\leq I(W_1, W_2; Y^n) - I(W_1, W_2; Z^n) + \epsilon_n \quad (115)$$
$$\leq I(W_1, W_2; Y^n) - I(W_1, W_2; Z^n) + \epsilon_n$$
$$+ I(X_1^n, X_2^n; Y^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n|W_1, W_2) \quad (116)$$
$$= I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + \epsilon_n \quad (117)$$

where (115) is due to Fano's lemma [7], (116) is obtained by using (114), and (117) is a consequence of the fact that given (X_1^n, X_2^n), (W_1, W_2) is independent of the channel outputs.

Appendix VI
Proof of Theorem 7

We prove Theorem 7 in two parts, starting with achievability. User i $(i = 1, 2)$ generates $2^{n(R_i+\tilde{R}_i)}$ length-n codewords $\mathbf{X}_i$ through $\mathcal{N}(0, P_i\mathbf{I})$ and labels them $\mathbf{X}_i(w_i, \tilde{w}_i)$ where $w_i \in \{1, \ldots, 2^{nR_i}\}$, $\tilde{w}_i \in \{1, \ldots, 2^{n\tilde{R}_i}\}$. Here, R_i denotes the rate of the information-carrying messages and $\tilde{R}_i$ is the rate sacrificed to confuse the eavesdropper to achieve secrecy for user $i = 1, 2$. For example, if w_i is the message to be transmitted, user i selects a $\tilde{W}_i$ randomly and transmits $\mathbf{x}_i(w_i, \tilde{w}_i)$. Furthermore, these rates satisfy

$$R_i + \tilde{R}_i \leq \frac{1}{2}\log(1 + P_i), \qquad i = 1, 2 \quad (118)$$
$$\tilde{R}_i \leq \frac{1}{2}\log(1 + h_i P_i), \qquad i = 1, 2 \quad (119)$$
$$\tilde{R}_1 + \tilde{R}_2 = \frac{1}{2}\log(1 + h_1 P_1 + h_2 P_2) \quad (120)$$

Since interference gains, α, β, satisfy (47), each user can decode both other user's messages and its own message with vanishingly small probability of error [6]. Hence, we only need to show that this scheme yields perfect secrecy. To this end, we consider joint secrecy condition which is sufficient to ensure that secrecy constraints on the individual messages are satisfied [3]. We have,

$$H(W_1, W_2|Z^n)$$
$$= H(W_1, W_2, Z^n) - H(Z^n) \quad (121)$$
$$= H(W_1, W_2, X_1^n, X_2^n, Z^n) - H(X_1^n, X_2^n|W_1, W_2, Z^n)$$
$$- H(Z^n) \quad (122)$$
$$= H(W_1, W_2) + H(X_1^n, X_2^n|W_1, W_2) + H(Z^n|X_1^n, X_2^n)$$
$$- H(X_1^n, X_2^n|W_1, W_2, Z^n) - H(Z^n) \quad (123)$$
$$= H(W_1, W_2) + H(X_1^n, X_2^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n)$$
$$- H(X_1^n, X_2^n|W_1, W_2, Z^n) \quad (124)$$

where (123) is obtained by using the chain rule and the fact that given (X_1^n, X_2^n), (W_1, W_2) and Z^n are independent. We now consider each term of (124) separately. Since given (W_1, W_2), (X_1^n, X_2^n) can take $2^{n(\tilde{R}_1+\tilde{R}_2)}$ different values uniformly, we have

$$H(X_1^n, X_2^n|W_1, W_2) = n(\tilde{R}_1 + \tilde{R}_2) \quad (125)$$
$$= \frac{n}{2}\log(1 + h_1 P_1 + h_2 P_2) \quad (126)$$

The third term of (124) is bounded as

$$I(X_1^n, X_2^n; Z^n) \leq \frac{n}{2}\log(1 + h_1 P_1 + h_2 P_2) \quad (127)$$

due to the fact that i.i.d. Gaussian signalling achieves the capacity of a memoryless Gaussian channel. Finally, we bound the last term of (124). To this end, assume that eavesdropper is decoding (X_1^n, X_2^n) given (W_1, W_2). Since $\tilde{R}_1$ and $\tilde{R}_2$ are selected to lie in the capacity region of the MAC between the users and the eavesdropper, the error probability of this decoding is vanishingly small, implying

$$H(X_1^n, X_2^n|W_1, W_2, Z^n) \leq \epsilon_n \quad (128)$$

due to Fano's lemma. Plugging (126), (127), (128) into (124), we get

$$H(W_1, W_2|Z^n) \geq H(W_1, W_2) - \epsilon_n \quad (129)$$

Thus, this scheme yields perfect secrecy. After eliminating $\tilde{R}_1$ and $\tilde{R}_2$ from (118), (119) and (120), one can get the achievable region of Corollary 3. Hence, we complete the achievability part.

For the outer bound, we note that this channel satisfies the conditions in (6)-(7) and consequently, following similar lines as in the proof of Theorem 4, one can get the outer bound given in this theorem. Moreover, we can show the sum secrecy capacity for the case $h_1 + h_2 < 1$ by using the proof technique developed for Theorem 5 in Appendix IV.

References

[1] A. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, Jan. 1975.

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

[3] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. Submitted to *IEEE Trans. Inf. Theory*, May 2006.

[4] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[5] M. H. M. Costa and A. El Gamal. The capacity region of the discrete memoryless interference channel with strong interefence. *IEEE Trans. Inf. Theory*, IT-33(5):710–711, Sep. 1987.

[6] A. Carleial. A case where interference does not reduce capacity. *IEEE Trans. Inf. Theory*, IT-21(5):569–570, Sep. 1975.

[7] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley & Sons, 2006. 2nd edition.

[8] M. Madiman and A. Barron. Generalized entropy power inequalities and monotonicity properties of information. *IEEE Trans. Inf. Theory*, 53(7):2317–2329, Jul. 2007.

[9] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:623–656, Oct. 1948.

[10] N. M. Blachmann. The convolution inequality for entropy powers. *IEEE Trans. Inf. Theory*, 11(2):267–271, Apr. 1965.