Secrecy Capacity Region of the Gaussian Multi-Receiver 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 consider the Gaussian multi-receiver wiretap channel and evaluate its secrecy capacity region. This evaluation requires the identification of underlying auxiliary random variables. For this purpose, we first visit the converse proof of the scalar Gaussian broadcast channel, and show that this proof cannot be extended to this secrecy context. The failure of this extension comes from the insufficiency of the entropy-power inequality to resolve the ambiguity regarding the auxiliary random variables. Instead, we provide two converse proofs. The first one uses the alternative representation of the mutual information as an integration of the minimum-mean-square-error (MMSE) along with the properties of the MMSE. The second one uses the relationship between the differential entropy and the Fisher information via the de Bruin identity along with the properties of the Fisher information.**

I. Introduction

We consider the Gaussian multi-receiver wiretap channel, and provide a converse for its secrecy capacity region. The Gaussian multi-receiver wiretap channel consists of one transmitter, K legitimate receivers, and one eavesdropper[1]. The transmitter would like to send independent confidential messages to each user, while the eavesdropper listens to the ongoing communication between the transmitter and the legitimate receivers. Each communication link between the transmitter and the receivers is an additive Gaussian channel.

As we will show in the sequel, any Gaussian multi-receiver wiretap channel can be regarded as a degraded multi-receiver wiretap channel, whose secrecy capacity region is known in a single-letter form [4]–[6]. This single-letter expression involves auxiliary random variables which need to be identified to establish the secrecy capacity region. Since a direct evaluation of this single-letter expression is difficult, an immediate approach might be to obtain computable outer bounds. For the scenario without an eavesdropper, i.e., for the Gaussian scalar broadcast channel, the difficulty of finding the optimal auxiliary random variable was alleviated via a joint use of the entropy-power inequality [7], [8] and Fano's inequality by Bergmans in [9], where Bergmans did not use the single-letter formula for the capacity region. Later, El Gamal gave an alternative approach which uses only the entropy-power inequality [7], [8] to establish the capacity region starting from the corresponding single-letter formula [10]. Despite their differences, these two converses have an important common feature, which is that, both of them use the entropy-power inequality [7], [8] to identify the optimal auxiliary random variable.

As a natural approach, one might try to adopt the converse proof techniques of the scalar Gaussian broadcast channel [9], [10] to this secrecy context. However, in this paper, we first show that, existing converse techniques for the Gaussian broadcast channel, i.e., the converse proofs of Bergmans [9] and El Gamal [10], cannot be extended in a straightforward manner to provide a converse proof for the Gaussian multi-receiver wiretap channel. In fact, we explicitly show that the main ingredient of these two converses in [9], [10], which is the entropy-power inequality [7], [8], is not sufficient to conclude a converse for the secrecy capacity region.

Though the entropy-power inequality is insufficient to provide a converse proof for the Gaussian multi-receiver wiretap channel, we are able to prove the secrecy capacity region using different techniques. In particular, we provide two converse proofs. The first one uses the connection between the minimum-mean-square-error (MMSE) and the mutual information along with the properties of the MMSE [11], [12]. In additive Gaussian channels, the Fisher information and the MMSE have a complementary relationship in the sense that one of them determines the other one, and vice versa [13]. Thus, the converse proof relying on the MMSE has a counterpart which replaces the MMSE with the Fisher information in the corresponding converse proof. Hence, the second converse uses the connection between the Fisher information and the differential entropy via the de Bruin identity [7], [8] along with the properties of the Fisher information.

After the inclusion of this paper into the conference program, we generalized our results presented here. In particular, we establish the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel for the most general case, i.e., when the transmitter and each receiver, including the eavesdropper, is equipped with an arbitrary number of antennas. These new results are reported in [1], [2].

II. Degraded Multi-Receiver Wiretap Channels

We first revisit the degraded two-user multi-receiver wiretap channel. This channel consists of one transmitter with an input alphabet $\mathcal{X}$, two legitimate receivers with output alphabets $\mathcal{Y}_k$,

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

[1]Throughout this paper, we consider the case $K = 2$. For generalization to $K > 2$, please refer to [1], [2]. The secrecy capacity of the Gaussian wiretap channel, i.e., the case where $K = 1$, was established in [3].

$k = 1, 2$, and an eavesdropper with output alphabet $\mathcal{Z}$. The transmitter sends a confidential message to each user, say $w_k \in \mathcal{W}_k$ to the kth user, and all messages are to be kept secret from the eavesdropper. The channel is memoryless with a transition probability $p(y_1, y_2, z|x)$.

A $(2^{nR_1}, 2^{nR_2}, n)$ code for this channel consists of two message sets, $\mathcal{W}_k = \{1, \ldots, 2^{nR_k}\}$, $k = 1, 2$, an encoder $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, two decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k \to \mathcal{W}_k$, $k = 1, 2$. The probability of error is defined as $P_e^n = \max_{k=1,2} \Pr\left[g_k(Y_k^n) \neq (W_k)\right]$. A rate pair (R_1, R_2) is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{k\in\mathcal{S}(W)} R_k, \quad \forall\ \mathcal{S}(W) \tag{1}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_1, W_2\}$. Hence, we consider only perfect secrecy rates. The secrecy capacity region is defined as the closure of all achievable rate tuples.

The degraded two-user multi-receiver wiretap channel exhibits the following Markov chain

$$X \to Y_1 \to Y_2 \to Z \tag{2}$$

The secrecy capacity region of the degraded multi-receiver wiretap channel was established in [5], [6] for an arbitrary number of users and in [4] for two users.

Theorem 1 *The secrecy capacity region of the degraded two-user multi-receiver wiretap channel is given by the union of the rate tuples (R_1, R_2) satisfying*

$$R_1 \leq I(X; Y_1|U) - I(X; Z|U) \tag{3}$$
$$R_2 \leq I(U; Y_2) - I(U; Z) \tag{4}$$

where the union is over all probability distributions $p(u, x)$ such that

$$U \to X \to Y_1 \to Y_2 \to Z \tag{5}$$

III. Gaussian Multi-receiver Wiretap Channel

The Gaussian multi-receiver wiretap channel is defined by

$$Y_k = X + N_k, \quad k = 1, 2 \tag{6}$$
$$Z = X + N_Z \tag{7}$$

where the channel input X is subject to a power constraint $E\left[X^2\right] \leq P$. The variances of the zero-mean Gaussian random variables N_1, N_2, N_Z are given by $\sigma_1^2, \sigma_2^2, \sigma_Z^2$, respectively, and satisfy the following order

$$\sigma_1^2 \leq \sigma_2^2 \leq \sigma_Z^2 \tag{8}$$

Since the correlations among N_1, N_2, N_Z have no effect on the secrecy capacity region, we can adjust the correlation structure to ensure that the following Markov chain is satisfied

$$X \to Y_1 \to Y_2 \to Z \tag{9}$$

Thus, this channel can be considered as a degraded channel, and its secrecy capacity region is given by Theorem 1. Hence, to compute the secrecy capacity region explicitly, we need to find the optimal joint distributions of (X, U) in Theorem 1. The corresponding secrecy capacity region is given by the following theorem.

Theorem 2 *The secrecy capacity region of the two-user Gaussian SISO wiretap channel is given by the union of the rate pairs (R_1, R_2) satisfying*

$$R_1 \leq \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_Z^2}\right) \tag{10}$$
$$R_2 \leq \frac{1}{2}\log\left(1 + \frac{\bar{\alpha} P}{\alpha P + \sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{\bar{\alpha} P}{\alpha P + \sigma_Z^2}\right) \tag{11}$$

where the union is over all $\alpha \in [0, 1]$, and $\bar{\alpha}$ denotes $1 - \alpha$.

The achievability of this region can be shown by selecting (X, U) to be jointly Gaussian in Theorem 1. We focus on the converse proof in the rest of the paper.

IV. Insufficiency of the Entropy-Power Inequality

We now show that a straightforward extension of the existing converse proofs for the Gaussian broadcast channel in [9], [10] is insufficient to provide a converse proof for the Gaussian multi-receiver wiretap channel. In particular, what we will show is that a stand-alone use of the entropy-power inequality [7], [8], which is the main tool in the converse proofs of Bergmans [9] and El Gamal [10], falls short of proving the optimality of Gaussian (X, U) in this secrecy context, as opposed to the Gaussian scalar broadcast channel. For that purpose, we consider El Gamal's converse for the Gaussian scalar broadcast channel. However, since the entropy-power inequality is in a central role for both El Gamal's and Bergmans' converses, the upcoming analysis can be done by using Bergmans' proof as well.

First, we consider the bound on the second user's secrecy rate. Using (4), we have

$$\begin{aligned} I(U; Y_2) - I(U; Z) = &\left[I(X; Y_2) - I(X; Z)\right] \\ &- \left[I(X; Y_2|U) - I(X; Z|U)\right] \end{aligned} \tag{12}$$

where the right-hand side is obtained by using the chain rule, and the Markov chain $U \to X \to (Y_1, Y_2, Z)$. The expression in the first bracket is maximized by Gaussian X [3] yielding

$$I(X; Y_2) - I(X; Z) \leq \frac{1}{2}\log\left(1 + \frac{P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{13}$$

Moreover, using the Markov chain $U \to X \to Y_2 \to Z$, we can bound the expression in the second bracket as

$$0 \leq I(X; Y_2|U) - I(X; Z|U) \tag{14}$$
$$\leq I(X; Y_2) - I(X; Z) \tag{15}$$
$$\leq \frac{1}{2}\log\left(1 + \frac{P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{16}$$

which implies that for any (X,U) pair, there exists an $\alpha \in [0,1]$ such that

$$I(X;Y_2|U) - I(X;Z|U) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \quad (17)$$

Combining (13) and (17) in (12) yields the desired bound on R_2 given in (11).

From now on, we focus on obtaining the bound given in (10) on the first user's secrecy rate. To this end, one needs to solve the following optimization[2]

$$\max \; I(X;Y_1|U) - I(X;Z|U) \quad (18)$$

$$\text{s.t.} \quad I(X;Y_2|U) - I(X;Z|U) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \quad (19)$$

When the term $I(X;Z|U)$ is absent in both the objective function and the constraint, as in the case of the Gaussian scalar broadcast channel, the entropy-power inequality [7], [8] can be used to solve this optimization problem. However, the presence of this term complicates the situation, and a stand-alone use of the entropy-power inequality [7], [8] does not seem to be sufficient. To substantiate this claim, let us consider the objective function in (18)

$$\begin{aligned} &I(X;Y_1|U) - I(X;Z|U) \\ &= h(Y_1|U) - h(Z|U) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \quad (20) \\ &\le \frac{1}{2}\log\left(1-\frac{2\pi e\left(\sigma_Z^2-\sigma_1^2\right)}{e^{2h(Z|U)}}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \quad (21) \end{aligned}$$

where the inequality is obtained by using the entropy-power inequality. Since the right-hand side of (21) is monotonically increasing in $h(Z|U)$, to show the optimality of Gaussian signalling, we need

$$h(Z|U) \le \frac{1}{2}\log 2\pi e(\alpha P + \sigma_Z^2) \quad (22)$$

which will result in the desired bound on (18), i.e., the desired end-result in (10).

We now check whether (22) holds under the constraint given in (19). To this end, consider the difference of mutual informations in (19)

$$\begin{aligned} &I(X;Y_2|U) - I(X;Z|U) \\ &= h(Y_2|U) - h(Z|U) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \quad (23) \\ &\le \frac{1}{2}\log\left(1-\frac{2\pi e\left(\sigma_Z^2-\sigma_2^2\right)}{e^{2h(Z|U)}}\right) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \quad (24) \end{aligned}$$

[2]One can consider the maximization of $I(X;Y_1|U)-I(X;Y_2|U)$ instead of the one in (18), while keeping the constraint in (19) the same. However, this alternative optimization would also yield a similar contradiction.

where the inequality is obtained by using the entropy-power inequality. Now, using the constraint given in (19) in (24), we get

$$\frac{1}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_Z^2}\right) \le \frac{1}{2}\log\left(1-\frac{2\pi e\left(\sigma_Z^2-\sigma_2^2\right)}{e^{2h(Z|U)}}\right) \quad (25)$$

which implies

$$\frac{1}{2}\log 2\pi e(\alpha P+\sigma_Z^2) \le h(Z|U) \quad (26)$$

Thus, as opposed to the inequality that we need to show the optimality of Gaussian signalling via the entropy-power inequality, i.e., the bound in (22), we have an opposite inequality. This discussion reveals that if Gaussian signalling is optimal, then its proof cannot be deduced from a straightforward extension of the converse proofs for the Gaussian scalar broadcast channel in [9], [10]. Thus, we need a new technique to provide the converse for Theorem 2. We next present two different proofs in the next two sections.

V. Converse for Theorem 2 Using the MMSE

We now provide a converse which uses the connection between the MMSE and the mutual information established in [11], [12]. In [12], the authors also give an alternative converse for the scalar Gaussian broadcast channel. Our proof will follow this converse, and generalize it to the context where there are secrecy constraints.

First, we briefly state the necessary background information. Let N be a zero-mean unit-variance Gaussian random variable, and (U,X) be a pair of arbitrarily correlated random variables which are independent of N. The MMSE of X when it is observed through U and $\sqrt{t}X+N$ is

$$\mathrm{mmse}(X,t|U) = E\left[\left(X - E\left[X|\sqrt{t}X+N,U\right]\right)^2\right] \quad (27)$$

As shown in [11], [12], the MMSE and the conditional mutual information are related through

$$I(X;\sqrt{t}X+N|U) = \frac{1}{2}\int_0^t \mathrm{mmse}(X,t|U)dt \quad (28)$$

For our converse, we need the following proposition which was proved in [12].

Proposition 1 ([12], Proposition 12) *Let U,X,N be as specified above. The function*

$$f(t) = \frac{\sigma^2}{\sigma^2 t+1} - \mathrm{mmse}(X,t|U) \quad (29)$$

has at most one zero in $[0,\infty)$ unless X is Gaussian conditioned on U with variance σ^2, in which case the function is identically zero on $[0,\infty)$. In particular, if $t_0<\infty$ is the unique zero, then $f(t)$ is strictly increasing on $[0,t_0]$, and strictly positive on (t_0,∞).

We now give the converse. We use exactly the same steps from (12) to (17) to establish the bound on the secrecy rate of the second user given in (11). To bound the secrecy rate of

the first user, we first restate (17) as

$$I(X;Y_2|U) - I(X;Z|U) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \quad (30)$$

$$= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \frac{\alpha P}{t\alpha P+1}dt \quad (31)$$

Furthermore, due to (28), we also have

$$I(X;Y_2|U) - I(X;Z|U) = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \mathrm{mmse}(X,t|U)dt \quad (32)$$

Comparing (31) and (32) reveals that either we have $\mathrm{mmse}(X,t|U) = \alpha P/(t\alpha P+1)$ for all $t \in [1/\sigma_Z^2, 1/\sigma_2^2]$, or there exists a unique $t_0 \in (1/\sigma_Z^2, 1/\sigma_2^2)$ such that

$$\mathrm{mmse}(X,t_0|U) = \frac{\alpha P}{t_0\alpha P+1} \quad (33)$$

and

$$\mathrm{mmse}(X,t|U) \leq \frac{\alpha P}{t\alpha P+1} \quad (34)$$

for $t > t_0$, because of Proposition 1. The former case occurs if X is Gaussian conditioned on U with variance αP, in which case we arrive at the desired bound on the secrecy rate of the first user given in (10). If we assume that the latter case in (33)-(34) occurs, then, we can use the following sequence of derivations to bound the first user's secrecy rate

$$I(X;Y_1|U) - I(X;Z|U) = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U)dt \quad (35)$$

$$= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \mathrm{mmse}(X,t|U)dt + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U)dt \quad (36)$$

$$= \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U)dt \quad (37)$$

$$\leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \frac{\alpha P}{t\alpha P+1}dt \quad (38)$$

$$= \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \quad (39)$$

where (37) follows from (31) and (32), and (38) is due to (34). Since (39) is the desired bound on the secrecy rate of the first user given in (10), this completes the converse proof.

VI. Converse for Theorem 2 Using the Fisher Information

We now provide an alternative converse which replaces the MMSE with the Fisher information in the above proof. We first provide some basic definitions. The unconditional versions of the following definition and the upcoming results regarding the Fisher information can be found in [14].

Definition 1 *Let X, U be arbitrarily correlated random variables with well-defined densities, and $f(x|u)$ be the corresponding conditional density. The conditional Fisher information of X is defined by*

$$J(X|U) = E\left[\left(\frac{\partial \log f(x|u)}{\partial x}\right)^2\right] \quad (40)$$

where the expectation is over (U,X).

The following conditional form of the Fisher information inequality [8] is proved in [2].

Lemma 1 *Let X, Y, U be random variables such that density for any combination of them exists. Moreover, assume that given U, X and Y are independent. Then, we have*[3]

$$J^{-1}(X+Y|U) \geq J^{-1}(X|U) + J^{-1}(Y|U) \quad (41)$$

Similarly, the following conditional form of the Cramer-Rao inequality is proved in [2].

Lemma 2 *Let X, U be arbitrarily correlated random variables with well-defined densities. Then, we have*

$$J(X|U) \geq \frac{1}{\mathrm{Var}(X|U)} \quad (42)$$

with equality if (U,X) is jointly Gaussian.

We now provide the conditional form of the de Bruin identity [7], [8], which is again proved in [2].

Lemma 3 *Let X, U be arbitrarily correlated random variables with finite second order moments. Moreover, assume that they are independent of N which is a zero-mean unit-variance Gaussian random variable. Then, we have*

$$\frac{dh(X+\sqrt{t}N|U)}{dt} = \frac{1}{2}J(X+\sqrt{t}N|U) \quad (43)$$

We now note the following complementary relationship between the MMSE and the Fisher information [11], [13]

$$J(\sqrt{t}X+N) = 1 - t\cdot\mathrm{mmse}(X,t) \quad (44)$$

which itself suggests the existence of an alternative converse which uses the Fisher information instead of the MMSE. We now provide the alternative converse based on the Fisher information. We first bound the secrecy rate of the second user as in the previous section, by following the exact steps from (12) to (17). To bound the secrecy rate of the first user, we first note that

$$I(X;Y_2|U) - I(X;Z|U) = -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U)dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \quad (45)$$

[3]Throughout the paper, $J^{-1}(\cdot)$ refers to $1/J(\cdot)$.

which follows from Lemma 3. We now bound the integrand in (45). For that purpose, we introduce two independent zero-mean unit-variance Gaussian random variables N', N'', which are also independent of (X, U). Then, we bound the integrand in (45) as follows

$$J^{-1}(X+\sqrt{t}N|U) = J^{-1}(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U) \tag{46}$$

$$\geq J^{-1}(X+\sqrt{t^*}N''|U) + J^{-1}(\sqrt{t-t^*}N'|U) \tag{47}$$

$$= J^{-1}(X+\sqrt{t^*}N''|U) + (t-t^*), \quad 0 \leq t^* \leq t \tag{48}$$

where (46) is due to the stability of Gaussian random variables, (47) is due to Lemma 1, and (48) follows from Lemma 2. The inequality in (48) is equivalent to

$$J(X+\sqrt{t}N|U) \leq \frac{J(X+\sqrt{t^*}N''|U)}{1+J(X+\sqrt{t^*}N''|U)(t-t^*)} \tag{49}$$

Taking $t^* \leq \sigma_2^2$, and using (49) in (45), we get

$$I(X;Y_2|U) - I(X;Z|U)$$
$$\geq -\frac{1}{2}\log\frac{1+J(X+\sqrt{t^*}N''|U)(\sigma_Z^2-t^*)}{1+J(X+\sqrt{t^*}N''|U)(\sigma_2^2-t^*)} - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{50}$$

We remind that we had already fixed the left-hand side of this inequality in (17). Comparison of (50) and (17) results in

$$J(X+\sqrt{t^*}N''|U) \geq \frac{1}{\alpha P + t^*}, \quad 0 < t^* \leq \sigma_2^2 \tag{51}$$

At this point, we compare the inequalities in (34) and (51). These two inequalities imply each other through (44) after appropriate change of variables and by noting that $J(aX) = (1/a^2)J(X)$ [14]. We now find the desired bound on the secrecy rate of the first user via using the inequality in (51)

$$I(X;Y_1|U) - I(X;Z|U)$$
$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U)dt - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{52}$$

$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U)dt$$
$$-\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U)dt - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{53}$$

$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U)dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right)$$
$$-\frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{54}$$

$$\leq -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2}\frac{1}{\alpha P+t}dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{55}$$

$$= \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{56}$$

where (54) follows from (45) and (17), and (55) is due to (51). Since (56) provides the desired bound on the secrecy rate of the first user given in (10), this completes the converse proof.

VII. Further Remarks

As mentioned in the introduction, in our new papers [1], [2], we generalized our results here to Gaussian MIMO multi-receiver wiretap channels which are defined by

$$\mathbf{Y}_k = \mathbf{H}_k\mathbf{X} + \mathbf{N}_k, \quad k = 1,\ldots,K \tag{57}$$

$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z \tag{58}$$

where the channel input $\mathbf{X}$, a $t \times 1$ column vector, is subject to the trace constraint $\mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P$. The kth user's observation is denoted by $\mathbf{Y}_k$ which is a column vector of size $r_k \times 1,\ k = 1,\ldots,K$. The eavesdropper's observation $\mathbf{Z}$ is of size $r_Z \times 1$. The covariance matrices of the Gaussian random vectors $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are $\{\mathbf{\Sigma}_k\}_{k=1}^K, \mathbf{\Sigma}_Z$, which are strictly positive definite. The channel gain matrices $\{\mathbf{H}_k\}_{k=1}^K, \mathbf{H}_Z$ are of sizes $\{r_k \times t\}_{k=1}^K, r_Z \times t$, respectively, and they are known to the transmitter, all legitimate users and the eavesdropper.

In [1], [2], we show that a variant of dirty-paper coding with Gaussian signals is optimal for these channels. To find the secrecy capacity region of the most general case in (57)-(58), we first obtain the secrecy capacity region of the degraded case, and raise this result to the general case by using channel enhancement and some limiting arguments [1], [2]. Our main contribution is the way we provide the converse proof for the degraded case, for which the Fisher information matrix plays a central role, as its scalar form did here.

References

[1] E. Ekrem and S. Ulukus. Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Globecom 2009*, Mar. 2009.

[2] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2009. Also available at [arXiv:0903.3096].

[3] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.

[4] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. The secrecy rate region of the broadcast channel. In *46th Annual Allerton Conf. Commun., Contr. and Comput.*, Sep. 2008. Also available at [arXiv:0806.4200].

[5] E. Ekrem and S. Ulukus. On secure broadcasting. In *42th Asilomar Conf. Signals, Syst. and Comp.*, Oct. 2008.

[6] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. Submitted to *EURASIP Journal on Wireless Communications and Networking*, Dec. 2008. Also available at [arXiv:0812.0319].

[7] A. J. Stam. Some inequalities satisfied by the quantities of information of Fisher and Shannon. *Information and Control*, 2:101–112, Jun. 1959.

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

[9] P. Bergmans. A simple converse for broadcast channels with additive white Gaussian noise. *IEEE Trans. Inf. Theory*, 20(3):279–280, Mar. 1974.

[10] A. El Gamal. EE478 Multiple user information theory. Lecture notes.

[11] D. Guo, S. Shamai (Shitz), and S. Verdu. Mutual information and minimum mean-square error in Gaussian channels. *IEEE Trans. Inf. Theory*, 51(4):1261–1283, Apr. 2005.

[12] D. Guo, S. Shamai (Shitz), and S. Verdu. Estimation of non-Gaussian random variables in Gaussian noise: Properties of the MMSE. In *IEEE ISIT*, Jul. 2008. Also submitted to *IEEE Trans. Inf. Theory.*

[13] O. Rioul. Information theoretic proofs of entropy power inequalities. Submitted to *IEEE Trans. Inf. Theory*, Apr. 2007. Also available at [arXiv:0704.1751].

[14] O. Johnson. *Information theory and the central limit theorem*. Imperial College Press, 2004.